NASA CONTRACTOR REPORT

NASA CR-2

NASA CR-2687

# INFORMATION AND DISPLAY REQUIREMENTS FOR INDEPENDENT LANDING MONITORS

*J. S. Karmarkar and J. A. Sorensen*

*Prepared by*
SYSTEMS CONTROL, INC.
Palo Alto, Calif. 94306
*for Langley Research Center*

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION • WASHINGTON, D. C. • AUGUST 1976

| | | |
|---|---|---|
| 1. Report No.<br>NASA CR-2687 | 2. Government Accession No. | 3. Recipient's Catalog No. |
| 4. Title and Subtitle<br>Information and Display Requirements for Independent Landing Monitors | | 5. Report Date<br>August 1976 |
| | | 6. Performing Organization Code |
| 7. Author(s)<br>J.S. Karmarkar and J.A. Sorensen | | 8. Performing Organization Report No. |
| | | 10. Work Unit No. |
| 9. Performing Organization Name and Address<br>SYSTEMS CONTROL, INC. (Vt)<br>1801 Page Mill Road<br>Palo Alto, CA 94306 | | 11. Contract or Grant No.<br>NAS1-13490 |
| | | 13. Type of Report and Period Covered<br>Final Report<br>July 1974 - July 1975 |
| 12. Sponsoring Agency Name and Address<br>National Aeronautics and Space Administration<br>Langley Research Center<br>Hampton, Virginia | | 14. Sponsoring Agency Code |

15. Supplementary Notes

Langley technical monitor: Patrick A. Gainer

Final report.

16. Abstract

The rising costs of air travel and the increased demand for consistent service has motivated providing avionics systems which enable all-weather landing capability. All-weather landing can be at least partially accomplished through provision of automatic landing (autoland) systems and improved landing aids such as the microwave landing system (MLS). The trend towards increased automation, together with increased equipment and maintenance costs, have motivated a rethinking of the potential role of the crew during automatic phases of flight. The problem, addressed in this study, concerns the ways an Independent Landing Monitor (ILM) may be used by the crew to complement the autoland function. In particular, a systematic procedure is devised to establish the information and display requirements of an ILM during the landing phase of the flight.

Functionally, the ILM system is designed to aid the crew in assessing whether the total system (e.g., avionics, aircraft, ground navigation aids, external disturbances) performance is acceptable, and, in case of anomaly, to provide adequate information to the crew to select the least unsafe of the available alternatives. Economically, this concept raises the possibility of reducing the primary autoland system redundancy and associated equipment and maintenance costs. The required level of safety for the overall system would in these cases be maintained by upgrading the backup manual system capability via the ILM.

A safety buget analysis is used to establish the reliability requirements for the ILM. These requirements are used as constraints in devising the fault detection scheme. Covariance propagation methods are used with a linearized system model to establish the time required to correct manually perturbed states due to the fault. Time-to-detect and time-to-correct requirements are combined to devise appropriate

| | |
|---|---|
| 17. Key Words (Suggested by Author(s))<br>Independent Landing Monitors<br>Human Pilot Model<br>Covariance Propagation | 18. Distribution Statement<br>Unclassified - Unlimited<br>Subject Category 04 |

| | | | |
|---|---|---|---|
| 19. Security Classif. (of this report)<br>Unclassified | 20. Security Classif. (of this page)<br>Unclassified | 21. No. of Pages<br>169 | 22. Price*<br>$6.25 |

*For sale by the National Technical Information Service, Springfield, Virginia 22161

## TABLE OF CONTENTS

## TABLE OF CONTENTS (CONTINUED)

# INFORMATION AND DISPLAY REQUIREMENTS FOR INDEPENDENT LANDING MONITORS

By J.S. Karmarkar and J.A. Sorensen
Systems Control, Inc.

## I. INTRODUCTION

There are major economic reasons for providing the capability of all-weather operations to most National Airspace users. The fact that airports are frequently closed or operating at reduced capacity because of low visibility is a primary source of lost revenue and increased operating cost. Prolonged holding patterns and diversions to alternate airports increase fuel usage, labor costs, and aircraft inefficiency. These delays also diminish user good will, and in some cases, cause the customer to seek alternate means of transportation. These economic considerations have motivated a concentrated effort on the part of the appropriate government agencies--National Aeronautics and Space Administration, the Federal Aviation Administration, and the Department of Defense--to sponsor the development of all-weather landing capability [1-4].

Increasing the number of IFR operations and improvements in IFR efficiency are being accomplished through the development of advanced onboard avionics (automatic landing system, Category III ILS). But using these advanced systems during low visibility implies that more precautions must be taken to ensure flight safety. In order for the pilot to accept fully the new equipment capability which allows him to land in low visibility conditions, he must be reasonably satisfied that his chances of safe landing are at least as great as under VFR conditions.

The ability of different users to pay different amounts for all-weather avionics equipment has resulted in varying degrees of

IFR landing capability in the respective aircraft fleets. These range from Category I (where there must be at least a 61 m (200 feet) altitude visibility ceiling) to Category IIIc (where the landing is essentially blind). Aircraft avionics must be certified to be allowed to land under each of these categories, and the certification procedures ensure that the appropriate measures of system safety (probability of catastrophic accident) are adequately met. For Category I conditions, the avionics must allow the pilot to get below 200 feet and be satisfactorily lined up with the runway for a manual landing. For Category IIIa operation, present landing systems have utilized automatic landing to pass certification requirements. To meet these requirements currently necessitates that the automatic landing (autoland) system have multiple component redundancy to guard against failure.

Avionics system improvements which have been suggested to improve all-weather landing capability include development of provisions for the following: (1) allow landing with lower visibility limits, and (2) use the pilot's monitoring ability to reduce the necessary complexity of the automatic landing systems. These desired improvements have produced the need for re-examination of the potential role of the Independent Landing Monitor (ILM). Such a device would obtain independent information about the state of the aircraft relative to the runway to allow the pilot to assess the performance of the landing operation.

The ILM actually has several envisioned uses and several associated configurations. The ILM uses include providing the crew with information to:

1. Allow lowering the visibility minimums while maintaining the present-day levels of safety.

2. Allow the pilot to determine whether an anomaly has occurred in the onboard guidance system or the ground-based ILS or MLS signal during the landing phase. This information includes the decision of whether manual landing or manual go-around should be attempted.

3. Guide the aircraft for manual landing or go-around in case of takeover during flight.

4. Guide the aircraft in case of fault during ground roll or takeoff.

5. Detect faults or pilot blunders during the approach phase.

Thus, the ILM can potentially improve aircraft operational economy by allowing more operations in low visiblity conditions and by reducing the required autoland equipment redundancy such that the initial investment and the recurring maintenance costs would be reduced. However, if the ILM is to be used to realize these cost savings, it must be shown that the resulting level of operational safety is at least equivalent to that of today's systems.

## Previous Developments

The previous work on the ILM has mainly focused on the development of sensors to provide a perspective view of the terrain ahead of the aircraft. The idea was that if an adequate display could be developed, this information could substitute for the normal visual cues such that a low visibility approach could be executed.

An early implementation of a landing monitor (for ILS approaches) was the Bendix Microvision System [5] tested on a C-131 at Wright-Patterson Air Force Base, Ohio in 1961. One of the main technical problems with the early Microvision System was that the system required the installation of active transponders on the runway surface, which would require international agreement and installation and maintenance costs. Secondly, to produce a coincident image of the runway, using a radar return stabilized by means of the existing commercial quality attitude gyroscopes, was technically impossible at that time. The distraction to the pilot of a runway image (formed by the transponders) moving around over the real world runway was more than enough, by itself, to discourage further development. Lastly, there was a growing awareness of the difficulty of providing pilot performance consistency to an adequately high confidence level.

The Lockheed ILM development utilizing a Texas Instruments radar [6] was based primarily upon the premise that pilot confidence in a completely automatic landing system for use in lower than Category II visibility might well need "boosting" by visibility enhancement of the runway. The purpose of the ILM was to provide high resolution radar mapping of the runway during Categories I, II, or III automatic approach and landings. The reason for landing monitor independence was to simplify the failure analysis by avoiding any interconnection between the ILM and the automatic approach and landing system. Moreover, the historically long time lapse between establishing a requirement for a new universal ground aid, its adoption by ICAO, and its universal implementation also encouraged independence. The Lockheed ILM concept was a go/no-go monitor for the autoland system rather than an independent flight director. Its intent was to allow the pilot to judge whether or not the landing was proceeding satisfactorily. The Lockheed ILM development was not completed partially because of indecision on its final role and benefits.

In contrast to the forward looking radar ILM developed for Lockheed, the concept [performance and failure assessment monitor (PAFAM)] proposed and implemented by McDonnell-Douglas was strictly a hardware monitor receiving inputs from the primary autoland system [7]. Based on internal models relating to the proper functioning of the key subsystems of the autoland system, the monitor made an assessment of the total performance and failure state of the aircraft system in terms of a predicted touchdown point. The underlying objective of this concept was to assist the pilot in making go/no-go decisions under pressure and in face of landing uncertainty. The goal of the system was to design the performance monitor to reduce the landing risk without imposing an unacceptable economic penalty in the number of aborted approaches. The PAFAM system, though conceptually attractive, has not met with wide acceptance by the airline industry. The principal difficulty lies in the fact that in the current implementation, it is very difficult to assure the integrity of the primary autoland system in the presence of existing interconnections with the PAFAM system.

During the course of other studies of the potential role and benefits of a perspective display as an ILM, simulator based experiments were conducted for each phase of flight in the terminal area [8]. These studies concluded that although a number of flight parameters are useful in assessing system performance, the usage of a perspective runway display is not essential.

## Objectives and Scope of Study

To determine if the ILM potential can be realized, it is eventually necessary to develop demonstration models for testing either in flight or in a cockpit simulator. To develop these models, it was first necessary to: (1) determine current and potential sensor capabilities, from a technological point-of-view, applicable to ILM mechanization, and (2) determine how sensor measurements should be processed in an ILM and displayed to the crew for flight evaluation. The first item (which was the subject of a separate study) will be combined with the second item (documented in this study report) to formulate ground based cockpit simulator experiments leading to ILM flight test.

The specific objectives of this study were as follows [2]:

(1) First, the various potential applications of an ILM were to be reviewed and reduced to a set that was most appropriate in terms of future development. The complete objective here was to define the ILM functions, and to determine the information (type and reliability) that is required by the pilot and crew for the realization of each of these functions.

(2) Next, various ways the ILM could be mechanized (in terms of sensor measurement processing and display) were to be considered. This required assessing different concepts of how faults could be detected, how the information could be displayed to pilot/crew, and what different crew procedures would be required to execute each of the flight options that the ILM could indicate.

(3) The final objective was to recommend which ILM concepts should be studied in further detail.

The first objective, defining the ILM applications, was done in terms of operational implications and hardware (sensors, processor, display) requirements. These definitions then allowed the ILM applications, which could be evaluated by analytical techniques (as opposed to cockpit simulator), to be selected for further study. These included providing: (1) backup fault monitoring of the primary autoland system, and (2) manual backup guidance in the event of a fault. The types of information possibly required in the ILM to mechanize these applications include:

(1) status of the aircraft states,
(2) whether a fault or anomaly has occurred,
(3) the type of anomaly,

(4) what action the pilot and crew should take, and
(5) guidance information for conducting that action.

The reliability requirements of this information were determined by conducting a safety analysis.

The second objective, determining how to mechanize these ILM applications, required conducting the following investigations:

(1) Determining how a fault could be detected and possibly discriminated from independent aircraft state measurements.

(2) Determining how long it takes to recovery manually from a perturbed condition after a fault has been detected.

(3) Determining the appropriate fault recovery strategy as a function of aircraft altitude.

(4) Specifying alternate ways this strategy and the associated guidance requirements could be displayed to the crew.

These investigative requirements thus formulated a systematic procedure for determining information and display requirements of the ILM and analyzing landing systems.

The approach used to conduct this study then consisted of five steps that were quite interrelated. These steps are shown as an iterative process by the flow chart shown in Figure 1. Before using this procedure, it was necessary to define (in terms of analytical models) elements of the aircraft/autoland/MLS/operating environment that need to be considered when developing the ILM. In addition, the possible uses of the ILM were defined in detail. However, the flight system and the terminal area flight profile are complex, and because of the limited effort possible, the study concentrated primarily on use of the ILM during the final landing portion of flight [300 m (1000 feet) altitude down to touchdown].

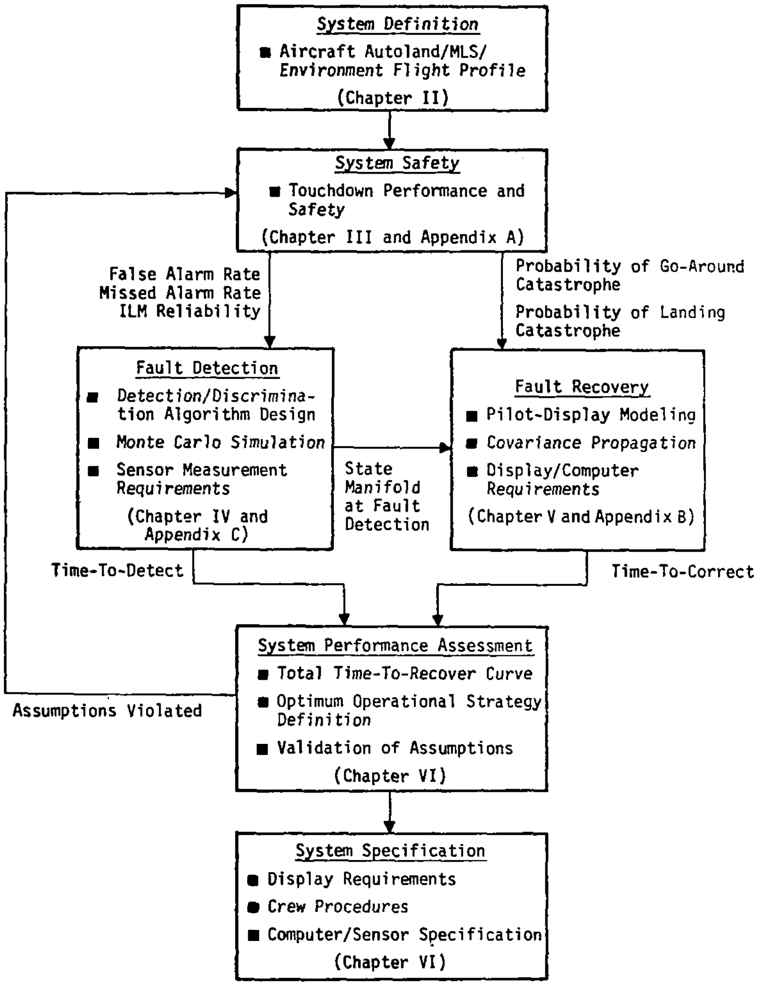

System Definition
■ Aircraft Autoland/MLS/ Environment Flight Profile
(Chapter II)
System Safety
■ Touchdown Performance and Safety
(Chapter III and Appendix A)
False Alarm Rate
Missed Alarm Rate
ILM Reliability
Probability of Go-Around Catastrophe
Probability of Landing Catastrophe
Fault Detection
■ Detection/Discrimination Algorithm Design
■ Monte Carlo Simulation
■ Sensor Measurement Requirements
(Chapter IV and Appendix C)
State Manifold at Fault Detection
Fault Recovery
■ Pilot-Display Modeling
■ Covariance Propagation
■ Display/Computer Requirements
(Chapter V and Appendix B)
Time-To-Detect
Time-To-Correct
System Performance Assessment
■ Total Time-To-Recover Curve
■ Optimum Operational Strategy Definition
■ Validation of Assumptions
(Chapter VI)
Assumptions Violated
System Specification
■ Display Requirements
■ Crew Procedures
■ Computer/Sensor Specification
(Chapter VI)

FIGURE 1. - OVERVIEW OF APPROACH USED TO ESTABLISH INFORMATION AND DISPLAY REQUIREMENTS OF AN INDEPENDENT LANDING MONITOR

With the operating scenario and flight system defined, specifying the constraints under which an ILM must operate was the first step of the analysis. The basic constraint is that landing safety must be preserved; the system using the ILM must improve landing capability with equivalent flight safety. The associated safety constraints on the ILM were determined using a probability tree with probabilities of different events (such as autoland fault, severe wind gusts, ILM failure) included. The result was a specification of the accuracy and reliability levels required for the ILM.

The initial function of the ILM is to detect system faults (autoland, MLS, or severe winds) such that the crew can be warned. Thus, the second step was to determine how the faults could be detected by ILM software and what the associated timing requirements (time-to-detect fault) were. This phase of the study used the safety budget values specified in the previous step.

After a fault has been detected, it is important to know how long it takes for manual recovery to allow a safe go-around or the continuation of the landing sequence. The third step of the study was to determine fault recovery time (time-to-correct) from various error states. This recovery time is fundamental to the determination of what crew strategy (go-around or continue the landing) should be used, given that a fault has been detected. The strategy is selected that yields the maximum safety on a probabilistic basis.

The fourth step was to combine time-to-detect and time-to-correct results to define the envelope around the landing flight path within which fault recovery is possible from a safety point-of-view. This envelope is used to determine from what altitudes fault recovery can be made safely and what the associated recovery strategy should be as a function of altitude. The third, fourth, and fifth steps just described define functionally the data processing requirements of the ILM, what measurements (ILM inputs) are necessary, how accurate the measurements should be, and what uses can be made of the ILM during the landing phase as a backup to automatic landing.

The fifth step of the study was to examine different ways the information from the ILM could be presented to the crew. Both alphanumeric (performance monitoring and fault recovery command)

and pictorial (aircraft state and guidance information) displays were considered. Associated crew procedures that would make use of these displays was also specified.

After these five steps were completed, a series of recommendations was made concerning what the next steps should be in investigating the potential of the ILM. Recommendations include the development of experimental ILM designs which are suitable for simulator and flight testing. The system description, the material developed in the five steps, and the resulting recommendations are the subjects of the next seven chapters of this report.

In summary, this report is organized as follows:

1. The second chapter presents the terminal area operating scenario in terms of economic factors, approach trajectories, navigation aids, aircraft types, avionics, and crew procedures. ILM application details and the main premises on which this study is based are also presented.

2. The third chapter presents the system safety budget analysis as a basis for: (a) justifying the incorporation of an ILM into the primary autoland system, (b) determining the fault detection equipment performance requirements, and (c) formulating the optimum post fault crew recovery procedure sequence (i.e., ILM strategy).

3. The fourth chapter discusses the investigation of fault detection and discrimination algorithms (consistent with the main premises of the study) to meet the system safety specifications previously generated. The specific algorithm studied in detail consists of a combination of the statistical chi-square ($\chi^2$) test and the Student's (t) test. Computer simulation results are presented to validate the analytical computations performed.

4. The fifth chapter deals with the fault recovery performance of the system using available pilot models and the covariance propagation technique. Starting with the system state manifold at fault detection, this phase of the study determines the recovery time required to bring the system state manifold within acceptable limits, from a safety point-of-view.

5. The sixth chapter brings together the safety budget, fault detection and discrimination, and fault recovery analyses to assess total time to recovery from a fault. The results are used to generate the ILM strategy (in terms of crew procedures) for the landing phase of flight. Then, two display configurations are presented which can be used to provide necessary information to the crew.

6. The seventh chapter summarizes the study results from the viewpoint of system safety, fault detection/discrimination, fault recovery, system implementation and ILM usage strategy. The main areas requiring further research are described, and a simulator/flight test validation plan is recommended.

7. Appendices A, B, and C present technical details used in the second through fifth chapters.

The reader who wishes to skip the study details can directly peruse the summary and conclusions presented in the seventh chapter.

# II. BACKGROUND

This chapter provides necessary background concerning the flight system and terminal area environment in which the ILM must operate. Also, different applications of the ILM are summarized, and specific applications studied in this effort are explained. The material in this chapter affects the methodology used throughout the study. Necessary subsystem details are discussed and definition of hardware and software constraints used to specify system requirements are given.

An overview is first given of the relationship of the elements in the flight system. Then, details are presented of the terminal area environment, associated crew procedures, autoland system considerations, and microwave landing system considerations. The ILM applications are presented in terms of what the corresponding general information and display requirements are. The operational implications of each application are listed, and justification is given for the specific applications evaluated in this study.

## Overview

The terminal area environment can be described in flow chart form as in Figure 2. The total system includes the aircraft, autoland system, aircraft state sensors, airborne displays, ground landing aids, air traffic control, the runway and surrounding terrain, wind, pilot, and the ILM. The ILM consists of airborne sensors, a data processor, associated displays and monitoring instrumentation, and possibly ground based aids.

Based on the command and advisory information presented to the pilot through cockpit displays, instruments, and monitors, either manual or automatic control of the aircraft is used. The pilot and

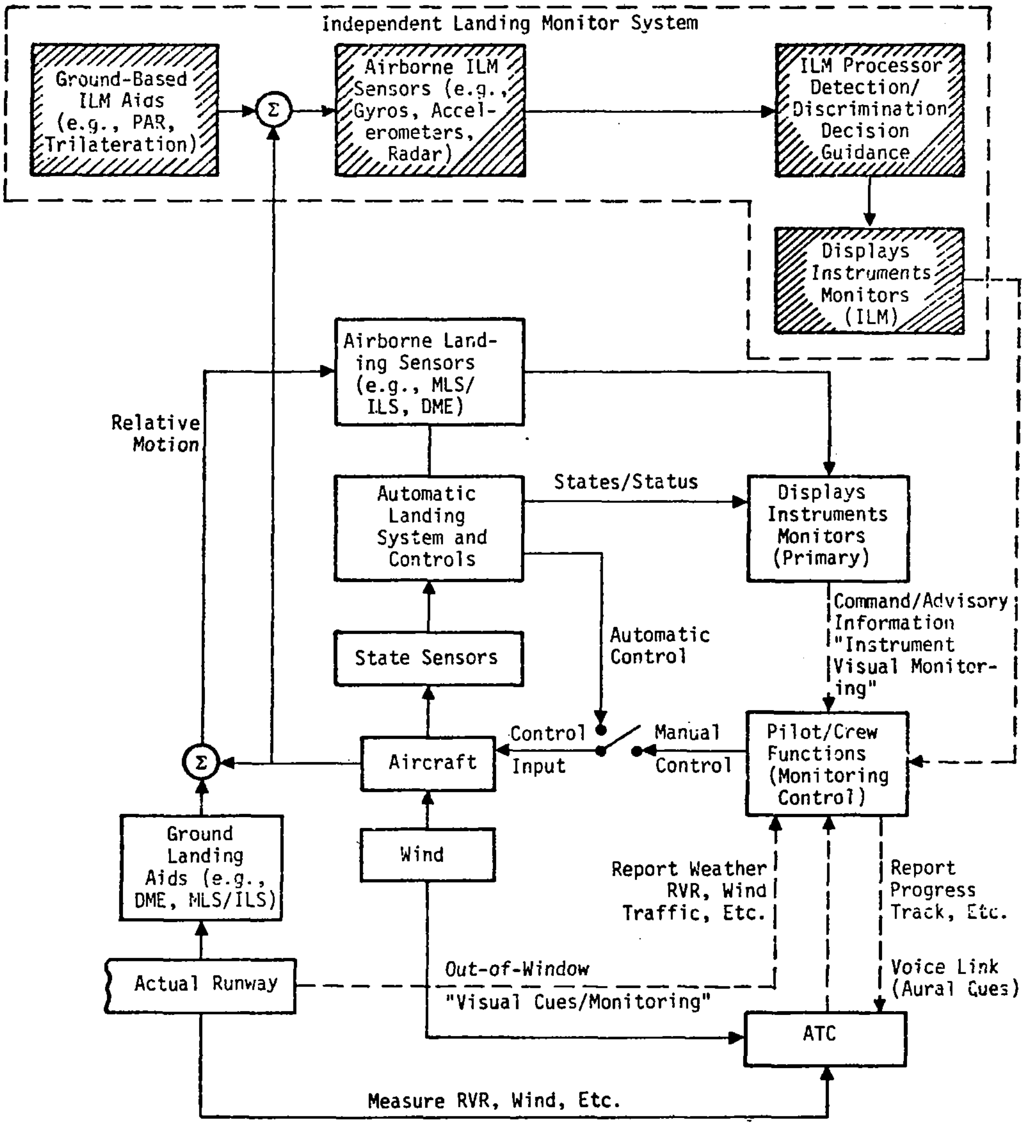

Independent Landing Monitor System
Ground-Based ILM Aids (e.g., PAR, Trilateration)
Σ
Airborne ILM Sensors (e.g., Gyros, Accelerometers, Radar)
ILM Processor Detection/ Discrimination Decision Guidance
Displays Instruments Monitors (ILM)
Airborne Landing Sensors (e.g., MLS/ ILS, DME)
Relative Motion
Automatic Landing System and Controls
States/Status
Displays Instruments Monitors (Primary)
Command/Advisory Information "Instrument Visual Monitoring"
Automatic Control
State Sensors
Σ
Aircraft
Control Input
Manual Control
Pilot/Crew Functions (Monitoring Control)
Ground Landing Aids (e.g., DME, MLS/ILS)
Wind
Report Weather RVR, Wind Traffic, Etc.
Report Progress Track, Etc.
Actual Runway
Out-of-Window "Visual Cues/Monitoring"
Voice Link (Aural Cues)
ATC
Measure RVR, Wind, Etc.

FIGURE 2.-TERMINAL AREA OPERATING SCENARIO - SYSTEM FLOW DIAGRAM

crew's decision making process is aided by vestibular motion cues and out-of-window visual cues. Under ceiling and visibility unlimited (CAVU) weather conditions, the pilot can execute a "successful" manual landing with these cues alone. On the other hand, under low visibility conditions, these cues are misleading and partially or totally lacking the required information content. The pilot and crew currently do not have display capabilities required for executing a "safe" manual landing under these conditions.

A "safe" manual landing is a process in which the probability of a catastrophic accident occurring is very small (e.g., $10^{-6}$). Technical details pertaining to this probabilistic analysis are developed in Appendix A. Because such a level of safety cannot be met when the aircraft is under manual control in low visibility, this has led to the development of the automatic landing system. Different types of autoland systems with different levels of redundancy and reliability have been developed, which are discussed shortly. Because different levels of reliability are present, each of these systems is certified to operate in different weather conditions. For example, an autoland system certified for Category II, will allow the aircraft to be automatically flown down to 30m (100 feet) altitude. At that point, the pilot must establish visual contact with the runway for monitoring purposes to allow the autoland to proceed with the landing or to execute a go-around. A Category III autoland system is certified to be operational down to touchdown.

Associated with each type of autoland system, there exists different applications of the Independent Landing Monitor. The benefits that these applications can produce are as follows:

1. Increased landing performance -- The ILM can compliment the autoland system such that landing can take place in lower visibility conditions than what the autoland system operating alone is certified for. This can be accomplished because the ILM provides additional monitoring capability of the flight system to the pilot. This increases the

level of safety and allows the aircraft to be flown automatically to a lower altitude before visual contact with the runway must be made.

2. Increased safety -- The ILM can be used to detect out-of-tolerance wind gusts or other aircraft on the runway that the autoland sensors cannot do. Thus, additional safety is provided to the system. In addition, these features serve the pilot as confidence builders in the autoland system.

3. Reduced redundancy -- Several autoland systems discussed later have a high degree of subsystem redundancy to ensure that the probability of failure in flight is acceptably low. To maintain this redundant equipment is expensive. The ILM can potentially reduce the required redundancy by taking advantage of the sensing and monitoring capabilities of the pilot and crew. By providing sufficient information to the crew, the ILM enables using a less redundant primary autoland; this reduces both the initial investment and the subsequent equipment maintenance costs.

Thus, there are three factors which must be considered when analyzing the ILM and its applications - landing performance, safety, and equipment redundancy. In the subsequent sections, the elements of Figure 2 are considered in terms of these three measures. These measures also dictate the constraints placed upon the information and display requirements for the Independent Landing Monitor.

## Terminal Area Environment And Crew Procedures

The terminal area environment can be described in a graphical fashion as in Figure 2. The total terminal area environment consists of the aircraft/autoland system with the associated airborne sensors for navigation and control, the ground based navigation aids (e.g., MLS, ILS), and the air traffic control system (ATC). The purpose of the ATC system is to schedule the aircraft in the landing queue, report pertinent data such as weather, runway visual range (RVR), wind and other traffic.

The number of terminal area parameters that in some way affect the ILM system concept is rather large. Table 1 summarizes the principal aspects of the terminal area flight path, atmospheric conditions, pilot/crew procedural considerations, landing characteristics and airport characteristics. These and other considerations must be investigated prior to the actual deployment of any ILM system.

Terminal area flight path.- A typical terminal area flight path consists essentially of an initial, intermediate and final approach segment as shown in Figures 3 and 4. A procedure turn is used to transition from the initial to the intermediate segment, as shown in Figure 3 [9]. The vertical profile for the final approach segment is depicted in Figure 4. This figure also shows the obstacle clearance line (OCL) and missed approach line (MAL), in the vertical plane, above which the aircraft must remain during the final approach and missed approach, respectively. The corresponding obstacle clearance slopes in the lateral plane are 12:1 with respect to the runway centerline for both approaches. These clearance requirements are related to the total system safety as discussed in the next chapter.

Under low visibility conditions, the roll out portion of the aircraft path must be considered with respect to roll out guidance and control. This phase of flight essentially involves a changeover from aerodynamic control to nose wheel control with the objective being to follow the runway centerline.

To conduct a detailed ILM requirements study, each portion of this flight path must be considered. For the purposes of the present study, it was considered adequate to model only the landing segment, shown in Figure 4. This is justified later. The methodology for conducting a detailed analysis of the entire terminal area flight profile is included in Appendix B.

TABLE 1.- TERMINAL AREA PARAMETERS

| ELEMENTS | PRINCIPAL ASPECTS |
|---|---|
| Terminal Area Flight Path | ● Landing Pattern (3D, 4D, Curved Decelerating)<br>● Special Flight Procedures (Procedure Turns, Merge Points)<br>● Ground Roll Procedures |
| Atmospheric Conditions | ● Steady Winds<br>● Wind Shear<br>● Wind Turbulence<br>● Altitude, Temperature, Pressure<br>● Snow, Fog, Visibility |
| Pilot/Crew | ● Aircraft Control Tasks<br>● Monitoring/Decision-Making<br>● Available Cues - Visual, Vestibular, Aural<br>● Other Work Items<br>● Crew Physical Status |
| Landing Characteristics (MLS, ILS, Lights) | ● Gain Variation and Offsets<br>● Transient Due to Overflights<br>● Ground Station Failures<br>● Light Pattern/Intensity |
| Airport Characteristics | ● Runway Gradients and Roughness<br>● Approach Terrain<br>● Runway Width, Length and Threshold Distance<br>● Tire-Runway Friction |

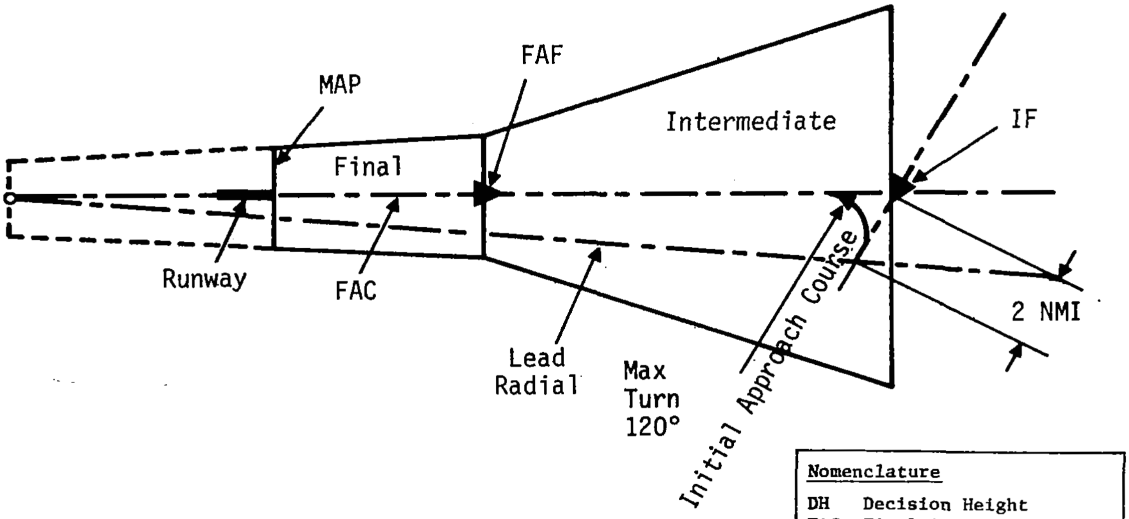


FIGURE 3.-TYPICAL TERMINAL AREA TRAJECTORY [9]

**Nomenclature**

| | |
|---|---|
| DH | Decision Height |
| FAC | Final Approach Course |
| FAF | Final Approach Fix |
| GPI | Ground Point of Intercept |
| IF | Intermediate Fix |
| MAL | Missed Approach Line |
| MAP | Missed Approach Point |
| MDA | Minimum Descent Altitude |
| OCL | Obstacle Clearance Line |
| OM | Outer Marker |
| TCH | Threahold Clearance Height |

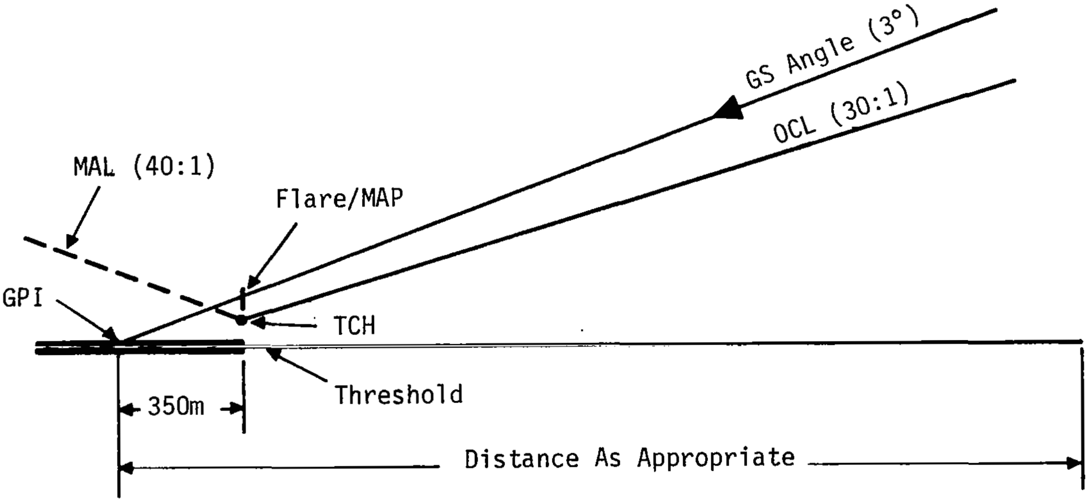


FIGURE 4.-TYPICAL FINAL APPROACH SEGMENT [9]

## Atmospheric Conditions

The certification requirements for commercial transport aircraft (FAR 25 and FAR 121) to operate under Category II and Category IIIa conditions have been defined by the FAA [10-12]. Terminal area operations in terms of runway availability and aircraft spacing are largely influenced by the weather category, as defined in Table 2 [9]. The airport weather category is determined mainly by the runway visual range (RVR), which is measured by ground based sensors and relayed to aircraft in the terminal area by the ATC system. Category IIIa also defines wind condition [12] limits and the corresponding touchdown parameter manifold denoting a "safe" landing [11, 12]; these are given in Tables 3 and 4, respectively. In the interest of comparison, the Category II window defined at decision height 30m (100 feet) is also noted in Table 4.

In order to establish that a given aircraft-autoland configuration meets the Category III requirements, in terms of landing safety, simulation studies are typically conducted to demonstrate that the touchdown manifold in Table 3 is not violated in a statistical sense [15]. Details pertaining to the requirements of these studies are presented in the next chapter and Appendix A.

To illustrate the frequency of Category II and Category III weather conditions for certain airport locations, a typical summary of reported weather conditions by landing category is given in Table 5 [14]. Based on his route structure, the airline operator can translate the performance improvement due to the incorporation of an ILM to reduce landing minima into increased revenues. This assumes that the ILM is highly reliable and that its use requires a minimum of maintenance and ground personnel training.

## TABLE 2.-ICAO ILS WEATHER CATEGORIES

| CATEGORY | RVR-M (FEET) | DECISION HEIGHT-M (FEET) | TIME TO TOUCHDOWN (SEC) |
|---|---|---|---|
| I | 723m (2400) | 61m (200) | 22-27 |
| II | 366m (1200) | 30.5m (100) | 12-15 |
| IIIa | 214m (700) | See to Rollout | 4-7 |
| IIIb | 46m (150) | See to Taxi | 0 |
| IIIc | 0 | Zero/Zero | 0 |

## TABLE 3.-CATEGORY III WIND CONDITION CONSTRAINTS

| QUANTITY | MAGNITUDE | | |
|---|---|---|---|
| Headwind | < 25 kts | | |
| Tailwind | < 10 kts | | |
| Croswind | < 15 kts | | |
| Turbulence (shear) | 8 kts/30.5m from 61m (200 feet) down to touchdown (TD) | | |
| Turbulence (gust) | u | v | w |
| Standard Deviations, kts (1σ) | .15 | .15 | 1.5 |
| Time Constant, Sec (V is airspeed in kts) | 600/V | 600/V | 30/V |

## TABLE 4.-CATEGORY III AND CATEGORY II PARAMETER MANIFOLD (1σ)

| QUANTITY | CATEGORY III TOUCHDOWN MANIFOLDS | CATEGORY II WINDOW |
|---|---|---|
| Longitudinal/Vertical | ± 76.3m (250 feet)/ - - - | - - - /± 3.66m (12 feet) |
| Lateral | ± 3.05m (10 feet) | ± 22m (72 feet) |
| Sink Rate | 0.61m/s (2 feet/s) | - - - |
| Lateral Speed/Forward Speed | ± 1.22m/s (4 feet/s)/ ± 2kts | - - - / ± 5kts |
| Crab Angle | ± 2° | - - - |
| Worst Case Longitudinal | 61.0m (200 feet) from threshold<br>< TD < 761m (2500 feet) from threshold | - - - |
| Worst Case Lateral | More than 1.52m (5 feet) from edge for 46m (150 feet) wide runway | - - - |

TABLE 5. - SUMMARY OF REPORTED WEATHER BY LANDING CATEGORY IN HOURS PER MONTH [14]

| | October 1970 | | November 1970 | |
|---|---|---|---|---|
| | Cat. II | Cat. III | Cat. II | Cat. III |
| Atlanta | 9 | 2 | 11 | 5 |
| Birmingham | 0 | 10 | 1 | 0 |
| Boston | 6 | 13 | 0 | 0 |
| Charlotte | 0 | 0 | 0 | 3 |
| Chicago O'Hare | 3 | 5 | 0 | 0 |
| Cleveland | 1 | 2 | 3 | 0 |
| Dallas Love | 3 | 0 | 0 | 0 |
| Detroit Metropolitan | 3 | 16 | 0 | 0 |
| Houston | 6 | 9 | 4 | 3 |
| Jacksonville | 0 | 0 | 6 | 0 |
| Los Angeles | 0 | 0 | 2 | 10 |
| New Orleans | 1 | 5 | 0 | 0 |
| New York Kennedy | 2 | 2 | 0 | 0 |
| Newark | 0 | 0 | 0 | 0 |
| Philadelphia | 0 | 0 | 0 | 0 |
| Pittsburgh | 2 | 6 | 6 | 16 |
| Portland | 11 | 15 | 10 | 5 |
| St. Louis | 4 | 0 | 0 | 2 |
| Seattle | 5 | 25 | 2 | 2 |
| Tampa | 0 | 0 | 0 | 6 |
| Washington National | 0 | 0 | 1 | 1 |

Time in hours is shown under Category II when the RVR is reported less than 732m (2400 feet) and equal to or greater than 366m (1200 feet). Time in hours is shown under Category III when the RVR is reported less than 366m. Data obtained from Eastern Airlines.

## Crew Procedures

As the aircraft proceeds automatically along the flight path depicted in Figures 3 and 4, the crew must monitor the operation of the autoland system. The set of discrete autoland actions that the crew must monitor is shown in Figure 5. The typical time sequence of flap, throttle, landing gear, decrab, flare and brake/spoiler deployment is presented in this figure. Simultaneously, the crew must also monitor whether the current state of the aircraft is acceptable. Typically, the crew is interested in flight path angle, vertical velocity, pitch attitude, slant range and range rate, velocity vector and cross track error and error rate. These have been graphically depicted in Figures 6a and 6b, respectively.

The onboard monitor and display subsystem of the typical autoland [16] normally provides the crew with status (autoland mode) and command (flight director mode) information. Additionally, the pilot and crew receive vestibular motion cues, possible out-of-window visual cues, and oral cues from the ATC system (Figure 2). Thus, based on information derived from many different sources, the pilot is required to make a judgement regarding the proper functioning of the elements of the primary autoland system. Clearly, this is a complex task which taxes the pilot's decision making capability even under clear visibility conditions. Under low visibility conditions (when the out-of-window visual cues are deficient, misleading, or totally lacking) when an upset occurs, the pilot simply cannot cope with the decision making and monitoring tasks. Here, he must be looking at all the cockpit instrumentation and deciding whether (a) the autoland was malfunctioning, (b) the external environment (e.g., wind gust) was unacceptable, or (c) the MLS signal was not within the specified category tolerances.

One potentially attractive approach to alleviating this information deficiency is to incorporate a system, operating independently from the primary guidance system, which would allow the pilot and crew to assess the performance of the autoland system, MLS, and

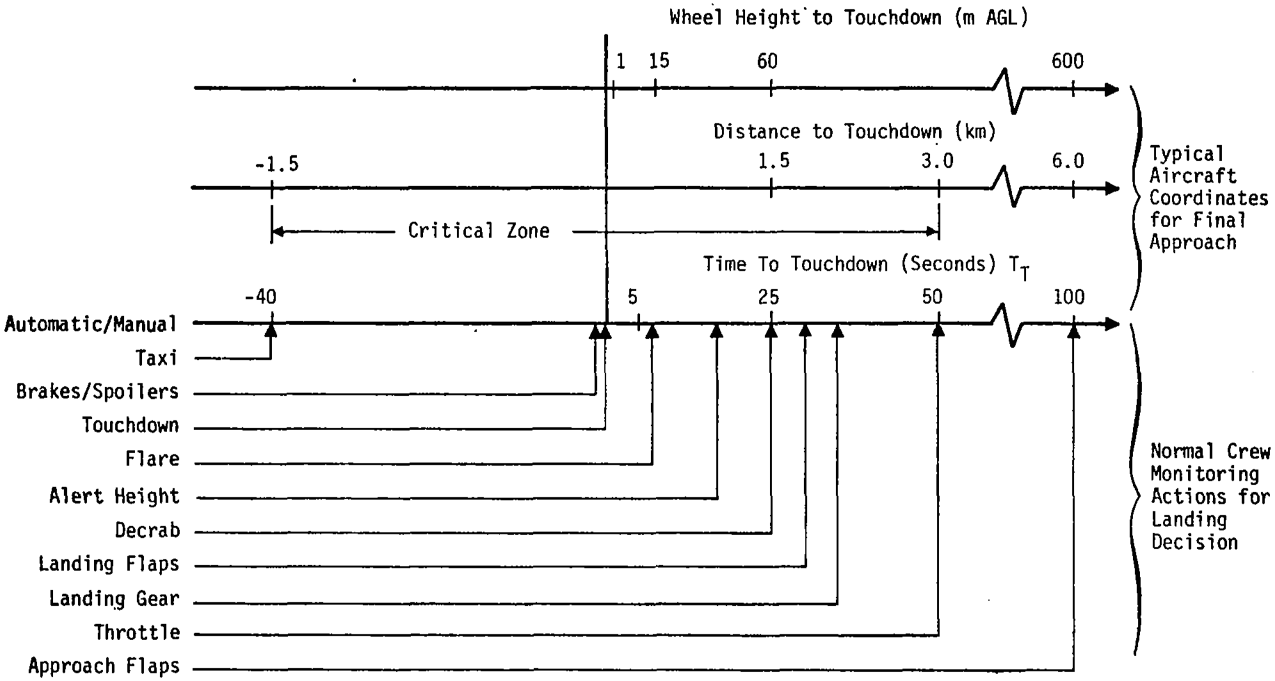
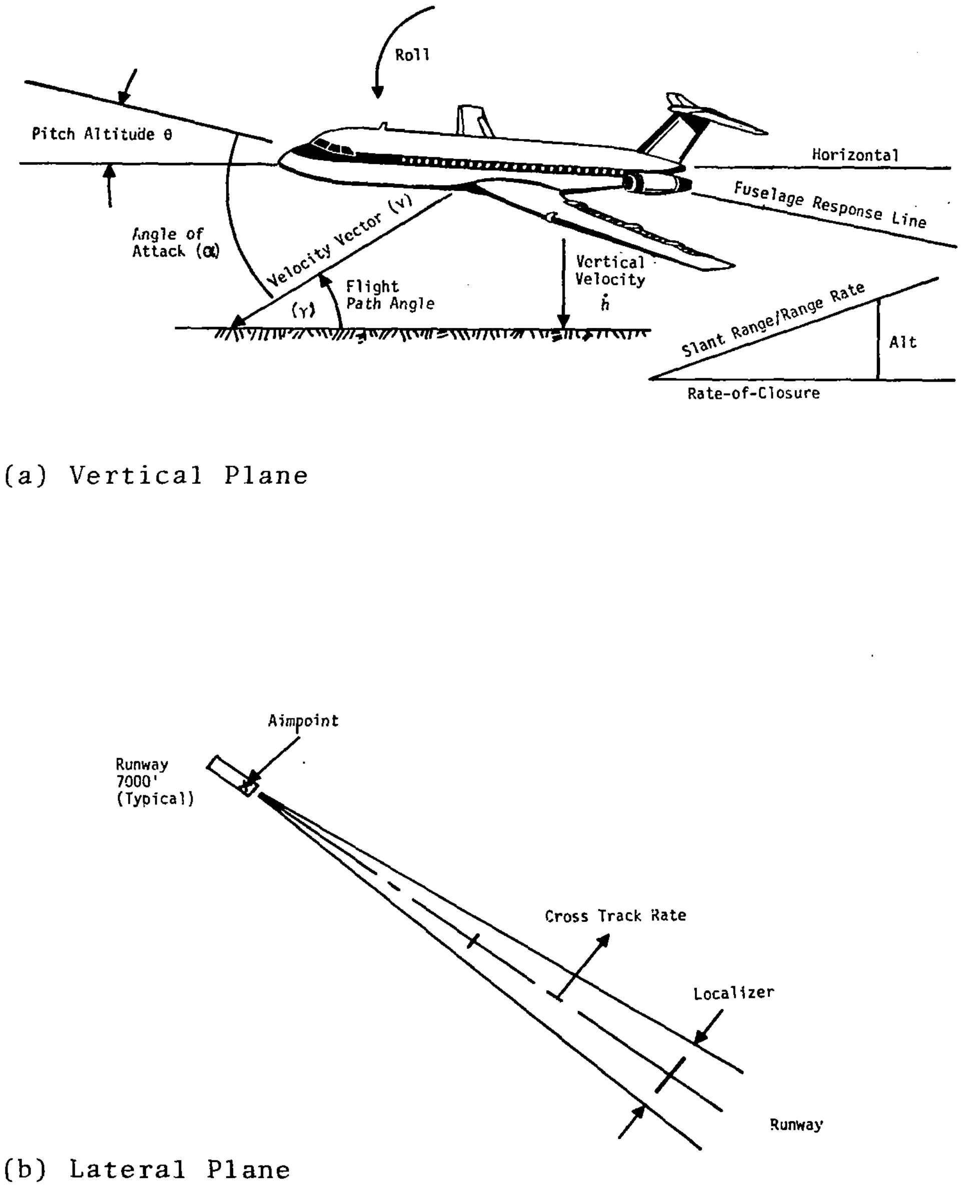

Wheel Height to Touchdown (m AGL)
1
15
60
600
Distance to Touchdown (km)
-1.5
1.5
3.0
6.0
Critical Zone
Time To Touchdown (Seconds) $T_T$
-40
5
25
50
100
Typical Aircraft Coordinates for Final Approach
Automatic/Manual
Taxi
Brakes/Spoilers
Touchdown
Flare
Alert Height
Decrab
Landing Flaps
Landing Gear
Throttle
Approach Flaps
Normal Crew Monitoring Actions for Landing Decision

FIGURE 5.-AUTOMATIC LANDING SEQUENCE



(a) Vertical Plane

(b) Lateral Plane

FIGURE 6.- ILLUSTRATION OF AIRCRAFT STATES MONITORED DURING THE LANDING APPROACH

external environment in terms of the aircraft's situation relative to the runway, under low visibility conditions. Such an independent landing monitor (ILM) system has been schematically presented by the shaded blocks in Figure 2. In addition to monitoring the current status of the aircraft, the ILM can have the capability of providing guidance commands to allow the pilot to execute a go-around, or to continue the landing sequence provided that the required levels of safety are maintained.

## Autoland System Considerations

The modern commercial aircraft under automatic control is an extremely complex system. To gain an appreciation of the complexity of such a system depicted at the center of Figure 2, the blocks representing the autoland system are redrawn in greater detail in Figure 7. The autoland system is a network of sensors/transducers, real time computational algorithms, control systems and actuators driving the aerodynamic surfaces. A partial list of the associated autoland sensors and transducers is given in Table 6.

The failure of one or more of these elements of the total avionics/autoland system, during the approach and landing phase of flight can result in a hazardous condition leading to a catastrophic outcome. Thus, to enhance the reliability of such a system, the entire system is generally duplicated and interconnected. A representative configuration, namely, triple modular redundancy (TMR), is depicted in Figure 8. This increased reliability is obtained at the expense of increased initial capital expenditure and recurring maintenance cost. Depending on the level of redundancy (e.g., dual, quadruple) and the redundancy management technique [17] (e.g., voting, hardware-aided software, etc.) the resulting avionics systems can continue to operate in spite of the total failure of one or more computers.

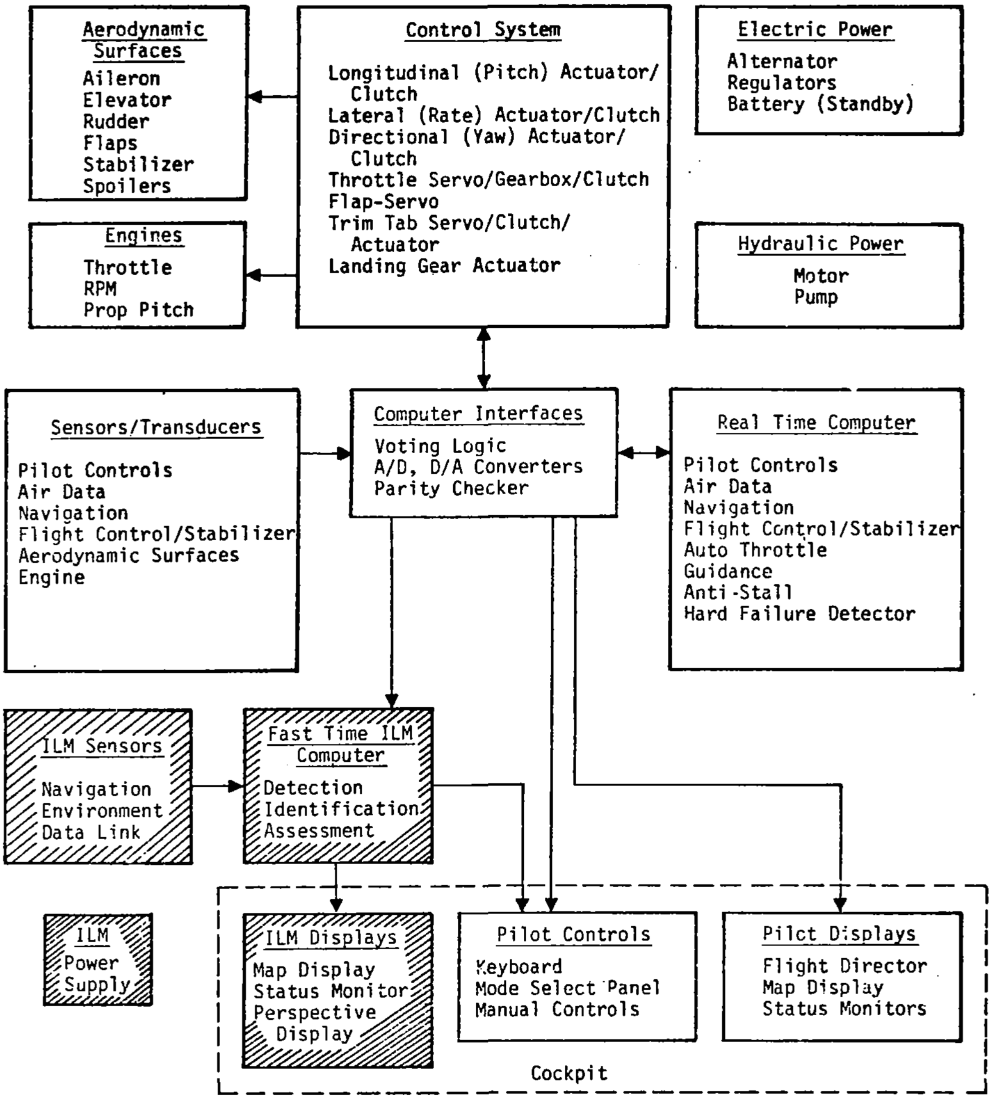


Figure 7.-AUTOLAND AIRBORNE HARDWARE BLOCK DIAGRAM (INCLUDING ILM)

TABLE 6.- AUTOLAND SENSORS/TRANSDUCERS (PARTIAL LIST)

| GENERAL CATEGORY | TYPES |
|---|---|
| Pilot Controls (Automatic) | Mode select panel, keyboard go-around switch, cut-out switch (computer) |
| Pilot Control (Manual) | Control wheel force (pitch/roll), trim switch |
| Air Data Transducers | Dynamic pressure, static pressure, air temperature, baro altimeter |
| Navigation Sensors | VHF Nav. receiver/controller/antenna, Tacan receiver/controller/antenna, radar altimeter, MLS receiver/controller/antenna, INS, ILS |
| Flight Control Stabilization Sensors | Vertical gyros, directional gyro, rate gyros, accelerometers, sideslip, angle-of-attack |
| Aerodynamic Surface Position Transducers | Elevator, aileron, rudder, flap, trim tab (elevator, aileron, rudder), spoilers |
| Engine Transducers | Throttle position, rpm, propeller pitch, oil pressure/temperature, exhaust gas temperature/pressure |

A "fail-operative" autoland system is a multiply redundant system that can detect a fault in any one of the redundant channels, automatically disconnect that channel, and continue to function properly. A "fail-passive" autoland system is a system with adequate redundancy to detect a fault in any one of the redundant channels and automatically disconnect the total system, leaving the aircraft in a safe condition for manual takeover. Typically, the autoland system must be fail operative to be certified for Category III operation. A fail-passive system is generally required for Category II certification. The type of system used governs the applications which are appropriate for consideration in conjunction with the autoland system.

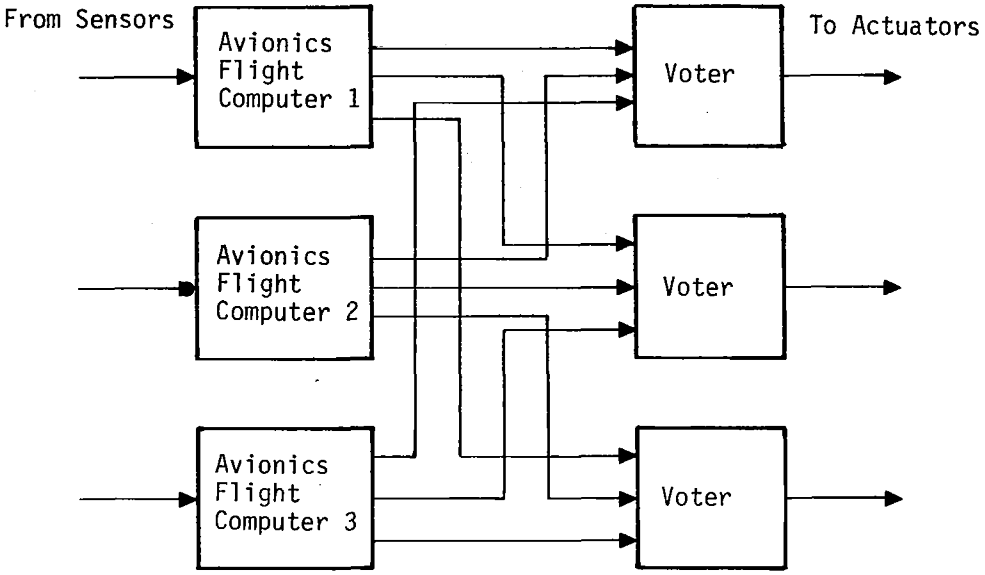

From Sensors
Avionics Flight Computer 1
Avionics Flight Computer 2
Avionics Flight Computer 3
Voter
Voter
Voter
To Actuators

FIGURE 8.-TRIPLE MODULAR REDUNDANCY CONFIGURATION

In designing autoland systems, built in monitors are added to detect the occurrence of component failures. Enough monitoring capability is added so that fixed levels of reliability (associated with the desired certification level) are achieved.

The methodology for deciding which failures are operationally significant, and the design of appropriate hardware monitors to detect these failures and take appropriate action is a complex, time-consuming, iterative design process referred to as Failure Mode and Effects Analysis (FMEA) [18]. This analysis consists of analyzing the signal characteristics at different points in each autoland subsystem to determine if the possible faults occurring in that subsystem can be detected fast enough to ensure that the aircraft cannot be upset to an unsafe attitude. The monitors are placed at the highest subsystem levels consistent with the reliability and fault detection speed desired. Hardware monitors provide signals indicating that failures have occurred, and they disconnect the failed subsystem.

The potential benefit of introducing an ILM system is to reduce the level of redundancy required and the degree of hardware monitoring. Normal system monitoring can be supplemented with ILM derived information to assess the functioning of the autoland system.

## Microwave Landing System Considerations

The United States and other countries are developing a new scanning beam Microwave Landing System (MLS), under the auspices of ICAO, to provide increased flexibility in precision landing [19]. The MLS will permit, through volumetric position information, advanced terminal approach paths such as two-segmented noise-abatement approaches, and curved decelerating flight paths. However, because of the complexity of these landing techniques, the pilot and crew's ability to monitor the approach progress and projected touchdown state will be more difficult than for the straight, flat, constant configuration and speed operations used with present-day Instrument Landing Systems (ILS).

The degree of trust which can be placed in the correctness of the information supplied by the MLS facility [21] is referred to as its integrity. The integrity requirement for MLS is as follows: When the system (ground/airborne) is operating in a "full up" Category III status, with no "abnormal" operating indications, the probability of both lateral and/or vertical guidance elements failing during the next 10 seconds (which can result in the radiation of a potentially hazardous guidance signal, or the loss of signal) will be less than $10^{-7}$.

Degradation of MLS data produces primarily "false course" or, more properly, "false position fixing" phenomena. Table 7 lists some of the major sources of MLS integrity degradation and correlates them to the type of integrity loss produced. The major environmental source of MLS integrity degradation is multipath effects. The major single approach to integrity assurance is again the use of hardware monitors. To mechanize a category III fail-operative ground system, a triplicate voting monitor system with fully redundant ground transmitters has been proposed. If the standby transmitter has been degraded beyond an acceptable course alignment tolerance, after it is on the air, an immediate shutdown will take place. During the time the standby transmitter is on the air, the facility category status will be downgraded and displayed to pilots and ATC. This will signal a suspension of Category III operations.

A foremost requirement for an all-weather landing system (such as the MLS) is the availability of complete fail-safe airborne integrity monitoring of the ground signal during the approach. In addition to alerting the pilot, it has been proposed that the flight control system be disconnected automatically in the case of the detected MLS equipment malfunctions. To achieve these requirements, dual processor integrity monitoring on each of the dual active airborne channels, along with an integral manual self test feature, has been recommended.

The level of redundancy built into the airborne and ground based portions of the Category III MLS, ensures low probability of failure, as stated earlier. Moreover, the hardware monitors built into the system informs the crew of malfunction within one second of occurrence. In the case of Category II MLS, the number of monitors

TABLE 7. - SOURCES OF MLS FAILURES AND THEIR SOLUTIONS [5]

| PROBLEM SOURCE | RESULTING PROBLEM SOLUTION | |
|---|---|---|
| | Bad Angle | Bad Auxiliary Angle |
| Degradation in MLS Ground Elements | | |
| Angle encoding error | FM,IM,RD | |
| Other coding malfunction | - | IM,RD |
| Sidelobe transmissions | SLS | - |
| Degradation By Environmental/ External Influences | | |
| Various multipath problems (terrain, obstacles, aircraft, etc.) | BC,AP | BF |
| Degradation by Spurious Signals | | |
| Interstation interference | AP | AP |
| Other RF sources | AP,BF | AP,BF |
| Degradation in MLS Airborne Elements | | |
| Receiver malfunction | PM,RD,BT | PM,RD,BT |

Solution Keys:

BF - Baseband format
RD = Redundancy
FM = Field monitoring
IM = Integral monitoring
BT = Built-in test

AP = Airborne processing
BC = Beam control (for multipath minimization)
SLS = Sidelobe suppression
SF = Scan format
PM = Airborne performance monitoring

and the redundancy level is reduced, so that the failure probability increases. The incorporation of an ILM into an airborne system can potentially allow Category III operation with a Category II MLS.

## ILM Application Areas

An ILM serving as a monitoring/warning aid must be able to detect and discriminate between (a) navigation degradation/failure, (b) autoland degradation/failure, (c) pilot blunder (e.g., miss set ILS or runway heading), (d) "out-of-design envelope" wind conditions, and (e) system failure of the ILM itself. As a guidance aid, the ILM must provide post-failure information to allow executing a manual takeover for go-around or landing, under low visibility conditions. From an economic standpoint, it must be ensured that adding an ILM to an already complex aircraft does not increase maintenance costs without a significant increase in overall system safety and all-weather performance. These requirements must be interpreted in terms of the application areas shown in Table 8.

On existing aircraft with single-channel autopilots, the ILM could reduce decision height and generate go-around commands on detecting an anomolous condition. On aircraft equipped with dual-channel autoland systems, an ILM of adequate integrity could be used to initiate a manual takeover to execute a landing or go-around depending on the nature of the fault and height of fault occurrence. It is noted that a perspective runway display is unnecessary as part of the ILM if its principal function is a fault monitor and/or go-around prompter.

On the other hand, if the objective is visibility enhancement or guidance to touchdown, then runway display becomes essential. Table 9 presents the ILM system functions, operational im-

TABLE 8.- APPLICATIONS OF INDEPENDENT LANDING MONITOR

| FUNCTION | FLIGHT PHASE | OPERATIONAL PERFORMANCE |
|---|---|---|
| Gross Fault Monitor | Approach | Detect RNAV/MLS fault or pilot Blunder. Command Manual Go-Around or landing. |
| Gross Fault Monitor | Landing | Detect MLS/Autoland fault. Command manual go-around or landing from lower decision height. |
| Visibility Enhancement | Landing | Detect high ground or runway obstruction. Command go-around. |
| Fault Monitor/Manual Guidance | Landing | Provide manual guidance for go-around or landing as backup to autoland system. |
| Lateral Guidance | Rollout/Takeoff | Keep aircraft centered. Detect turnoff. |
| Longitudinal Guidance | Rollout/Takeoff | Monitor aircraft performance. Command rollout/takeoff abort and initiate emergency procedures |

plications and associated information and display requirements, assuming a runway display is present. Proceeding from the top entry of the table to the bottom, the system requirements become increasingly sophisticated.

In any case, the key requirement for using an ILM is as follows: The system with the ILM must be demonstrated (and hence certifiable) to be as safe or safer than the system without an ILM under low visibility conditions. The methodology for establishing this requirement is the subject of the next chapter.

TABLE 9.-ILM SYSTEM FUNCTIONS AND IMPLICATIONS (ASSUMING RUNWAY DISPLAY CAPABILITY

|  |  | INFORMATION AND DISPLAY HARDWARE REQUIREMENTS |  |  |
|---|---|---|---|---|
| FUNCTIONAL REQUIREMENTS | OPERATIONAL IMPLICATIONS | SENSOR | PROCESSOR | DISPLAY |
| Gross Fault Monitor<br>Confidence Builder | •Increased Category IIIa Service<br>•Reduced Orientation Time In IFR Situations | •Minimal Resolution | •Decluttering | •Perspective Distance CRT<br>•Down/Up |
| Visibility Enhancement<br>High Ground and Runway Obstruction Detector | •Reduce Decision Height And Unnecessary Go-Around<br>•Avoid Ground Collisions | •Increase Field of View (FOV)<br>•Increased Resolution, FOV, and Scan Rate | •Same As Above<br>•Faster Processor | •Head up<br>•Same As Above |
| Lateral Rollout/Takeoff Guidance | •Safety Increase | •Increase Resolution, and Scan Rate | •Same As Above | •Same As Above |
| Longitudinal Rollout/Takeoff Guidance | •Safety Increase (Category IIIb | •Reduce Interference<br>•Additional Sensors Required (e.g., DME) | •Distance Computation | •Distance Display (Analog) |
| Manual Backup Guidance for Fail Passive Autoland<br>Fault Monitor Backup | •Upgrade Fail Passive Autoland Category II/IIIa<br>•Reduce Decision Height and Unnecessary Go-Arounds | •High Resolution, Scan Rate, and FOV<br>•Additional Sensors Required (e.g., Attitude Gyros, Altimeter) | •Distance<br>•Alignment<br>•Crab Angle<br>•Flight Path Angle<br>•Attitude Stability<br>•Ground Roll/Takeoff Distance | •Synthetic Display<br>•Symbol Generator |

## ILM Application Studied Under This Effort

As has been shown, there are many interrelated subsystems which affect the operation of the ILM. Because of the limited effort possible in this study, it was decided to concentrate on the automatic portion of the ILM system's potential. Referring to Table 9, it can be deduced that the ILM applications associated with having runway display capability (confidence builder, visibility enhancement, high ground and runway obstruction detector) can only be analyzed by cockpit simulator or flight test capability. For such studies, an ILM mockup or prototype would be necessary. Thus, these applications were only considered in terms of what general display requirements would be necessary.

Referring to Table 8, it was felt that the greater economic potential from the ILM can be realized during the landing phase. It is also in this phase that the ILM has the most critical effect on systems safety. Furthermore, if a methodology could be developed for determining information and display requirements for the landing phase, it would be straight forward to extend this methodology to analyze the approach and ground phases of flight.

Thus, the applications considered in detail were the automatic functions of the ILM during the landing phase of flight. These included fault monitoring/detection and manual guidance in the presence of a fault.

The ILM applications had to consider the nature of the autoland equipment on board. Because a fail-operative system (required for Category III operations) is supposed to be essentially failsafe, the ILM fault detection and guidance applications are more suited to aircraft with fail-passive or less sophisticated systems. A key question then was as follows: How much lower can the visibility ceiling be set when an ILM is being used, if the same level of safety is to be maintained as is present with the higher ceiling and no ILM? The approach presented in the following chapters directly addresses this question.

To answer this question required assessing the time-to-detect and correct a fault by use of an ILM and manual control. Total fault recovery time was used to define an altitude, namely, "critical altitude" below which no fault was recoverable within the desired levels of safety, for a go-around decision. Similarly, an altitude was determined below which no fault was safely recoverable for a landing decision; this altitude was labeled "decision altitude." Thus, decision altitude and critical altitude define switchover points in the decision strategy associated with monitoring and detecting a fault. The exact values of these altitudes thus play key roles in assessing the economic value of using an ILM for lowering landing minimum for less sophisticated autoland capability.

# III. SYSTEM SAFETY ANALYSIS

This chapter addresses a number of basic issues concerning use of the ILM that are affected by safety requirements. These are: (1) On what basis can existence and use of an ILM be justified? (2) How is the strategy associated with use of the ILM system affected? (3) On what basis will possible conflicting system failure indications of the autoland fault monitors be reconciled with those of the ILM? (4) What are the technical requirements (false alarm rate, missed fault rate) of the ILM fault detection equipment? and (5) What are the fault detection timing requirements?

The underlying means of addressing these pertinent questions is to analyze the contribution of subsystem reliability to overall system safety. In the process of answering these questions, an ILM system design methodology evolved, and it is presented in further detail in this chapter.

This chapter begins with an overview of safety and performance analysis which also includes aspects pertinent to certification. Then, ILM decision strategies and pilot takeover criteria are discussed. Numerical results are used to illustrate the interrelationship between safety and reliability. Then answers to the above questions are numerically illustrated. The mathematical details of the safety analysis are presented in Appendix B.

## Safety Analysis Overview

The overall design of advanced avionics/autoland systems (including an ILM for use in low visibility conditions [7, 9, 10 15]) requires consideration of two criteria--system performance and system safety. System performance is measured in terms of the statistical dispersion of the aircraft around the nominal state at touchdown (touchdown manifold). This is evaluated by considering the effects of variations within the normal equipment design tolerances (i.e., the effects of equipment faults are not considered) and normal external environment factors (i.e., turbulence, steady winds) on the touchdown dispersion manifold.

System safety assessment entails a more global consideration of the entire terminal area flight envelope. The effect of all faults and fault sequences within the system must be examined on a probabilistic basis to determine the total probability of exceeding specified flight path safety limits.

For the ILM, both system performance (touchdown manifold) and system safety (entire flight path envelope) must be assessed in terms of individual causes (e.g., design tolerances, turbulence, MLS beam bends, avionics faults and fault sequences, etc.) contributing to the overall probability of a catastrophic accident. This performance and safety analysis process is depicted in flow chart form in Figure 9. In this figure, fault-free performance is a measure of how often there is a catastrophic accident during landing even though the autoland system and associated equipment operate within normal tolerances. This probability is designated by $P_{nual}$. (The nomenclature is explained later.)

The "nuisance disconnect" (or false alarm") is a situation where, even though the primary autoland system is performing perfectly, the automatic system is disconnected because of some signal combination anomaly or hardware monitor failure. Then, manual takeover is required. Nuisance disconnect performance refers to the rate at which ensuing catastrophic accidents occur because of these false alarms. Here, the probabilities are designated by $P_{ndpl}$ and $P_{ndpg}$ which indicate that either a manual landing or a go-around was attempted when the accident occurs.

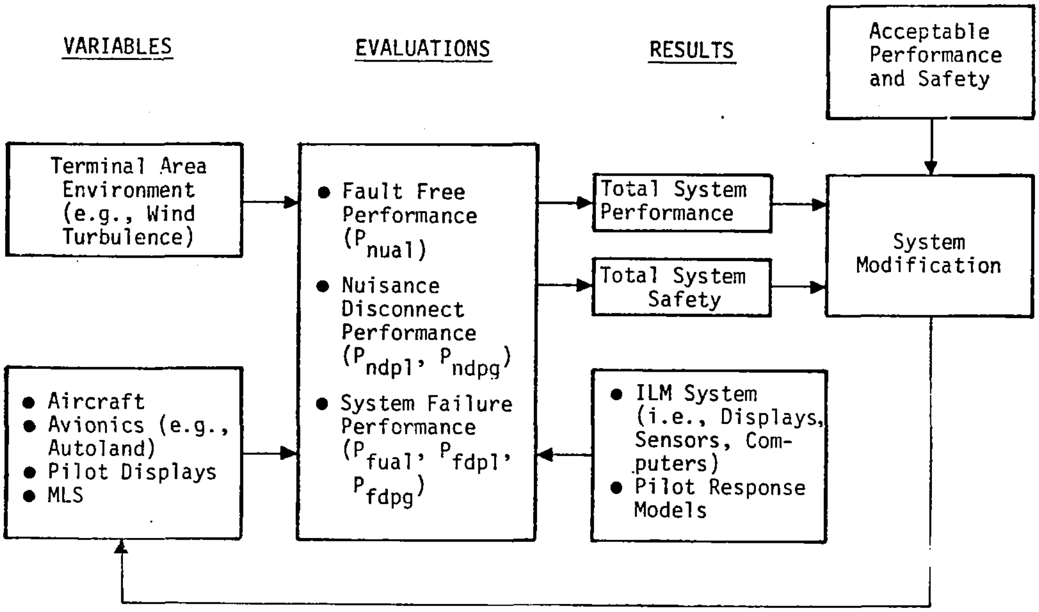

VARIABLES
EVALUATIONS
RESULTS
Acceptable Performance and Safety
Terminal Area Environment (e.g., Wind Turbulence)
● Fault Free Performance ($P_{nual}$)
● Nuisance Disconnect Performance ($P_{ndpl}$, $P_{ndpg}$)
● System Failure Performance ($P_{fual}$, $P_{fdpl}$, $P_{fdpg}$)
Total System Performance
Total System Safety
System Modification
● Aircraft
● Avionics (e.g., Autoland)
● Pilot Displays
● MLS
● ILM System (i.e., Displays, Sensors, Computers)
● Pilot Response Models

FIGURE 9.-FLOW CHART OF PROCESS REQUIRED FOR EVALUATION OF ILM SYSTEM SAFETY AND PERFORMANCE

A "system failure" may or may not be detected by the ILM or the primary system monitors. The rate of undetected failures that causes accidents is designated $P_{fual}$. The rates of detected failures followed by manual takeover that result in catastrophic accidents in landing or go-around are designated by $P_{fdpl}$ and $P_{fdpg}$, respectively.

To determine the ILM system's reliability requirements, each of these measures of performance must be known for the autoland system operating without the ILM. These probabilities are then combined and evaluated by using the overall safety requirement. The result is the determination of reliability requirements of the ILM system. Details of evaluating the fault free, nuisance disconnect, and system failure performance (together with the associated probability definitions) are discussed later in this chapter.

## System Performance Evaluation

As noted above, system performance is evaluated in terms of the touchdown dispersion envelope. The process of evaluating this performance typically consists of setting up a detailed computer simulation of the aircraft, avionics/autoland, landing aids, and the external environment [9]. Then, by performing an extensive Monte Carlo analysis, the fault free performance of the entire autoland system is evaluated in terms of the probability of catastrophic accident (aircraft state exceeds safety constraints).

Some of the terminal area parameters which must be incorporated into such a simulation are presented in the previous chapter. The external environment simulation model would include the wind conditions, such as those defined in Table 3. An example of the acceptable touchdown parameter manifold that would be used in testing is presented in Table 4.

If the overall system safety requirement is specified as an acceptably small rate of catastrophic accidents per number of landing attempts, then the fault-free performance measure must be a smaller subset of this overall rate. For example, the current overall safety criterion for certification of a Category III autoland system is that the catastrophic accident probability rate be less than $10^{-7}$. The contribution of the fault free autoland system to this number is specified to be no greater than $10^{-8}$. For a five dimensional terminal state manifold, this corresponds to the rate at which the seven sigma values computed from Table 4 are exceeded. (See Appendix B).

Performance failure during go-around (i.e., probability of a catastrophic accident while executing a go-around) must be evaluated by computer simulation in a manner similar to the landing evaluation. Clearly defined criteria similar to Table 4 are not available; this can be attributed to the fact that performance failures in go-around are highly aircraft dependent. In general, performance failures result from exceeding certain aerodynamic constraints (e.g., angle-of-attack, sideslip) or violation of obstacle clearance boundaries.

## System Safety Evaluation

The overall system safety assessment can be performed by defining an event outcome tree. Then, the probability of occurrence of each outcome leading to a catastrophy is determined by analysis and simulation. Some of the results may be validated by flight test. Finally, total system probability of catastrophic failure is determined by summing these probabilities, as defined by the outcome tree.

The failure rates are dependent upon the strategies that a pilot may take in case of a detected fault. In the following, two possible pilot strategies are first defined; then an event outcome tree is presented for one of these strategies. Subsequently, the incorporation of the ILM's reliability measures into this probability tree is discussed. The associated problem of resolving a possible conflict between the autoland and ILM monitor signals is then treated.

Pilot decision strategies.- Two distinct pilot decision strategies are feasible following the detection of an autoland system fault during the landing sequence. These are depicted in Figures 10 and 11. Consider an airborne system equipped with autoland capability but no ILM. Suppose that the autoland is engaged at height $h_0$; then, the first decision strategy, designated A, consists of executing a go-around if the autoland monitors detect a fault between altitude $h_0$ and h*. An emergency landing is executed if the fault is detected between h* and touchdown (TD). The value of

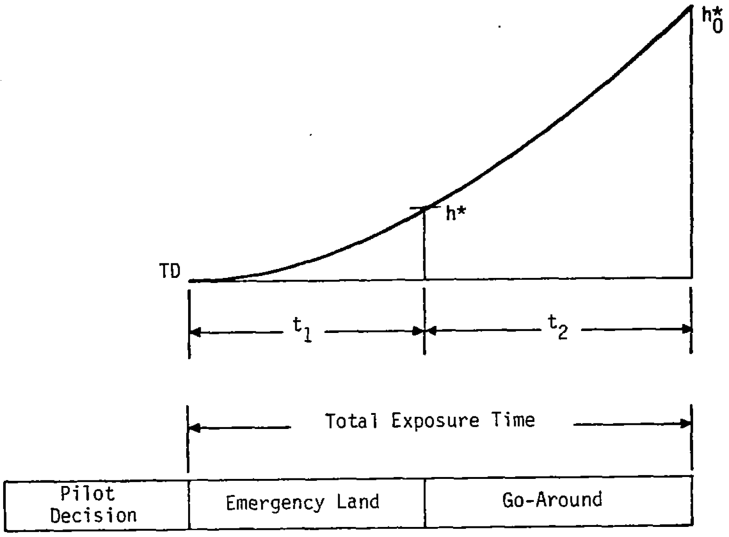


FIGURE 10. - POST FAULT DETECTION PILOT DECISION STRATEGY (A)

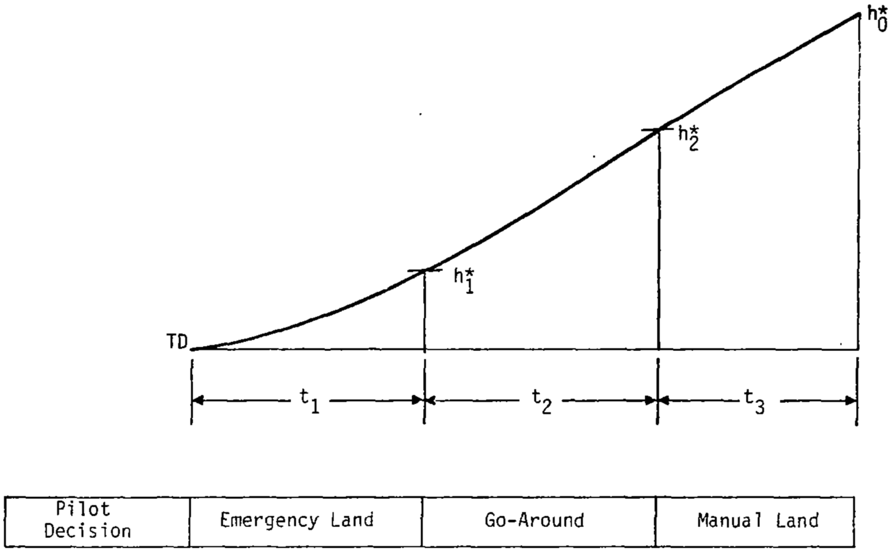


FIGURE 11. - POST FAULT DETECTION PILOT DECISION STRATEGY (B)

h* is determined statistically as the height above which it is safer to attempt a go-around in case of a fault. Below this altitude it is safer to attempt a manual landing. As shown in Figure 10, the nominal flight duration between these altitudes is $t_2$ and $t_1$, respectively.

The other possible strategy, shown in Figure 11, is to execute: (a) an emergency landing if the fault is detected between $h_1$* and TD, (b) go-around if the altitude of fault detection lies between $h_1$* and $h_2$*, and (c) execute a manual landing if the fault is detected between $h_o$ and $h_2$*. In this second strategy, $h_1$* is chosen in the same manner as h* in Strategy A. The higher altitude $h_2$* is chosen based on the assumption that above this altitude, there is adequate time to recover manually so that the landing sequence can safely be continued. Recovery consists of nulling out the state error caused by the fault and manually tracking the nominal approach flight path. It is noted that manual recovery for landing in Strategy B may be realistic only if visual contact can be established with the runway prior to $h_2$*. In other words, the visibility ceiling would not be below a minimum of $h_2$*. Alternatively, the ILM equipment must have the capability of providing manual guidance to touchdown.

Event outcome tree.- To illustrate the methodology of evaluating the total system probability of catastrophic accident, $P_A$, the outcome tree is now considered for an autoland with Strategy A depicted in Figure 12. The probability terms used in this figure are defined in Table 10. A detailed exposition of these probabilities is presented in Appendix B. These probability terms are essentially integrals of the associated probability density functions which must be determined in general by simulation methods. The hypothesized forms of the go-around and autoland catastrophe probability density functions are illustrated in Figures 13 and 14, respectively.

The branches of the tree in Figure 12 terminate with either landing or go-around failure probabilities. A landing failure can

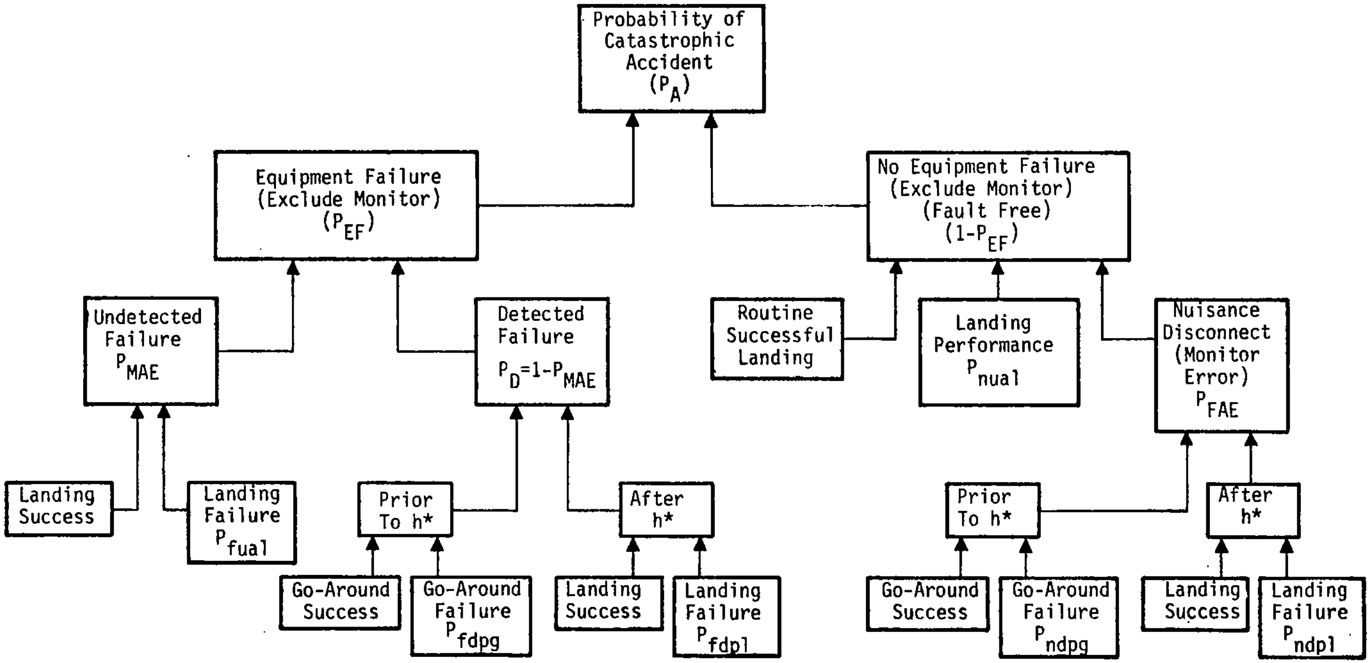

Probability of Catastrophic Accident ($P_A$)
Equipment Failure (Exclude Monitor) ($P_{EF}$)
No Equipment Failure (Exclude Monitor) (Fault Free) ($1-P_{EF}$)
Undetected Failure $P_{MAE}$
Detected Failure $P_D=1-P_{MAE}$
Routine Successful Landing
Landing Performance $P_{nual}$
Nuisance Disconnect (Monitor Error) $P_{FAE}$
Landing Success
Landing Failure $P_{fual}$
Prior To h*
After h*
Go-Around Success
Go-Around Failure $P_{fdpg}$
Landing Success
Landing Failure $P_{fdpl}$
Prior To h*
After h*
Go-Around Success
Go-Around Failure $P_{ndpg}$
Landing Success
Landing Failure $P_{ndpl}$

FIGURE 12. -EVENT OUTCOME TREE FOR MONITOR OPERATION DURING AUTOMATIC LANDING USING STRATEGY A.

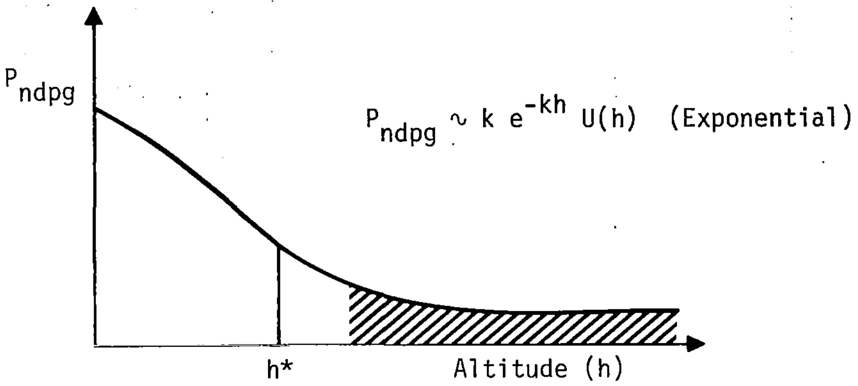


FIGURE 13. - PILOT RECOVERY CATASTROPHE PROBABILITY DENSITY FUNCTION

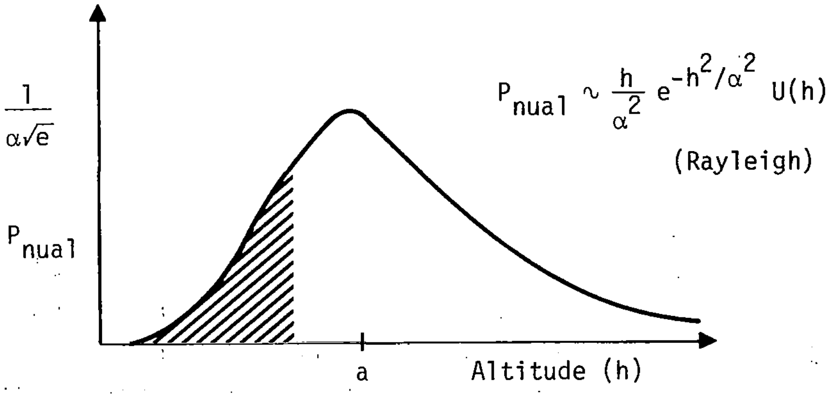


FIGURE 14. - AUTOLAND CATASTROPHE PROBABILITY DENSITY FUNCTION

## TABLE 10 . - OUTCOME TREE CATASTROPHE PROBABILITIES

| QUANTITY | EQUIPMENT FAILURE | MONITOR DETECTION | RESULTING PILOT OBJECTIVE | COMMENTS |
|---|---|---|---|---|
| $P_A$ | -- | -- | -- | Total System Probability of Catastrophe Accident |
| $P_{EF}$ | Yes | -- | -- | Probability of Equipment Failure |
| $P_{MAE}$ | Yes | No | -- | Probability of Missed Alarm Following Equipment Failure |
| $P_D$ | Yes | Yes | -- | Probability of Detected Fault |
| $P_{FAE}$ | No | Yes | -- | Probability of False Alarm Caused By Primary Equipment Monitors |
| $P_{nual}$ | No | No | Land | Fault Free Performance Measure |
| $P_{fual}$ | Yes | No | Land | Missed Alarm ($P_{MAE}$) |
| $P_{fdpg}$ | Yes | Yes | Go-Around | Prior to h* } detection $P_D = (1-P_{MAE})$ |
| $P_{fdpl}$ | Yes | Yes | Land | After h* |
| $P_{ndpg}$ | No | Yes | Go-Around | Prior to h* } nuisance disconnect false alarm $P_{FAE}$ |
| $P_{ndpl}$ | No | Yes | Land | After h* |

$P_{(f/n)(d/u)(p/a)(g/l)}$: probability of catastrophe

Notation:

| | |
|---|---|
| f - fault | p - pilot |
| n - no fault | a - automatic |
| d - detected | g - go-around |
| u - undetected | l - land |

h* - minimum descent altitude

occur due to a number of conditions which can be partitioned into the lateral and longitudinal failure effects. Lateral effects include such events as running off the side of the runway, excessive crab, and wing tip/pod/tail scrape. Longitudinal effects include overrunning the runway and hard/soft landing. Similarly, lateral go-around failure effects include violation of obstacle clearance and excessive roll angles and rates. Longitudinal go-around failures include such events as stall and unacceptable obstacle clearance.

On the basis of Figures 10 and 12, the total system probability of catastrophic accident, $P_A$, can be expressed as

$$P_A = P_{EF}\{P_{MAE}\ P_{fual} + (1-P_{MAE})(\alpha_1 P_{fdpl} + \alpha_2 P_{fdpg}) + \{1-P_{EF}\}\{P_{nual} + P_{FAE}\ (\alpha_1 P_{ndpl} + \alpha_2 P_{ndpg})\}. \tag{1}$$

Here, the exposure factors $\alpha_1$ and $\alpha_2$ are given by,

$$\alpha_1 = \frac{T_1}{(T_1 + T_2)} \tag{2}$$

$$\alpha_2 = \frac{T_2}{(T_1 + T_2)} \tag{3}$$

Basically, the exposure factor represents the portion of the total flight period during which the system is "exposed" to the consequences of a particular pilot decision.

Effect of an ILM on pilot takeover.- The incorporation of an ILM with its own monitors into an autoland system, brings up a significant operational problem. The source of the problem is the potential disagreement between the ILM and primary system monitor alarms. Table 11 lists the four takeover initiation options that could be used to resolve this situation. Clearly in an operational environment, one of these must be selected as being more appropriate. The logical way to resolve this conflict is to determine which of these four options leads to the highest level of system safety or lowest level of catastrophic accident probability, $P_A$. For a given autoland system, after having selected one of

TABLE 11.- POST-FAULT DETECTION PILOT TAKEOVER CRITERION OPTIONS

| OPTION | TAKEOVER INITIATION CRITERION |
|---|---|
| 1 | Consider Primary Monitors Only (i.e., no ILM) |
| 2 | Use Either ILM or Primary Monitors |
| 3 | Use ILM Only (i.e., Ignore Primary Monitors) |
| 4 | Use ILM and Primary Monitors (i.e., Act Only If Both Detect Fault) |

these options as the best, the pilot/crew would be trained to follow always that particular takeover criterion.

The combination of the two decision strategies presented in Figures 10 and 11 and the four takeover options listed in Table 11 result in eight design alternatives and eight associated accident probability equations for $P_A$. The generic form of the system safety equation is:

$$P_A = \{1-P_{EF}\}\{P_{nual} + w \cdot x\} + P_{EF}\{P_{fual}\, y + x \cdot z\} \qquad (4)$$

The parameters w, x, y and z for each of the eight combinations are expanded in terms of probability measures in Table 12. Detailed definitions of the probability measures are presented in Table 13. The equation pertaining to a specific strategy decision and initiation criterion is constructed by inserting the corresponding tabulated terms representing the false alarm rate, missed alarm rate, strategy, and initiation criterion. These equations form the basis for addressing the questions raised at the beginning of the chapter. The basic objective is to select the alternative that leads to the lowest probability of catastrophic accident $P_A$.

TABLE 12. -ACCIDENT PROBABILITY $P_A$ AS A FUNCTION OF DECISION STRATEGY AND INITIATION OPTION OPTION

$$P_A = \{1-P_{EF}\}\{\not{P}_{nual} + w \cdot x\} + P_{EF}\{\not{P}_{fual} \cdot y + x \cdot z\}$$

| DECISION STRATEGY | INITIATION CRITERION | w (FALSE ALARM) | x (STRATEGY) | y (MISSED ALARM) | z (CRITERION) | COMMENTS |
|---|---|---|---|---|---|---|
| A | 1 | $P_{FAE}$ | $P_{SAE} =$<br>$\alpha_1 P_{ELE} + \alpha_2 P_{GAE}$ | $P_{MAE}$ | $(1-P_{MAE})$ | |
| A | 2 | $P_{FAE} + P_{FAI}$ | $P_{SAI} =$<br>$\alpha_1 P_{ELI} + \alpha_2 P_{GAI}$ | $P_{MAE} \cdot P_{MAS}$ | $(1-P_{MAE})P_{MAI} +$<br>$(1-P_{MAS})P_{MAE} +$<br>$(1-P_{MAS})(1-P_{MAE})$<br>$= 1-P_{MAE} \cdot P_{MAS}$ | ● A Necessary Condition To Justify An ILM Is<br>$P_{ELI} << P_{ELE}$<br>$P_{GAI} << P_{GAE}$<br>$P_{ILM} \sim P_{MAI}$ |
| A | 3 | $P_{FAI}$ | $P_{SAI}$ | $P_{MAS} =$<br>$P_{ILM} + P_{MAI}$ | $(1-P_{MAS})$ | |
| A | 4 | $P_{FAI} \cdot P_{FAE}$ | $P_{SAI}$ | $P_{MAS}(1-P_{MAE}) +$<br>$P_{MAE}(1-P_{MAS})$ | $(1-P_{MAS})(1-P_{MAE})$ | |
| B | 1 | $P_{FAE}$ | $P_{SBE} = \alpha_1 P_{ELE}$<br>$+ \alpha_2 P_{GAE}$<br>$+ \alpha_3 P_{MLE}$ | $P_{MAE}$ | $(1-P_{MAE})$ | Visibility $P_{MLE}$<br>CAVU $10^{-6}$<br>CAT I $10^{-5}$<br>CAT II $10^{-3}$<br>CAT I 1(unacceptable) |
| B | 2 | $P_{FAE} + P_{FAI}$ | $P_{SBI} = \alpha_1 P_{ELI}$<br>$+ \alpha_2 P_{GAI}$<br>$+ \alpha_3 P_{MLI}$ | $P_{MAE} \cdot P_{MAS}$ | $(1-P_{MAE} \cdot P_{MAS})$ | ● A Necessary Condition To Justify This Strategy Is<br>$P_{MLI} << P_{MLE}$<br>and<br>$P_{MLI} < P_{GAI}$ |
| B | 3 | $P_{FAI}$ | $P_{SBI}$ | $P_{MAS}$ | $(1-P_{MAS})$ | |
| B | 4 | $P_{FAI} \cdot P_{FAE}$ | $P_{SBI}$ | $P_{MAS}(1-P_{MAE})$<br>$+ P_{MAE}(1-P_{MAS})$ | $(1-P_{MAS})(1-P_{MAE})$ | |

TABLE 13.-DEFINITION OF TERMS APPEARING IN TABLE 12

| QUANTITY | DEFINITION |
|---|---|
| $P_{FAE}$ | Probability Of False Alarm - Autoland/MLS/Other Equipment (Primary) Monitors |
| $P_{FAI}$ | Probability Of False Alarm - ILM |
| $P_{SAE}$ | Probability Of Catastrophe Using Strategy A With No ILM (Primary Monitors Only) |
| $P_{SAI}$ | Probability Of Catastrophe Using Strategy A With ILM |
| $P_{ELE}$ | Probability Of Emergency Landing Catastrophe With No ILM |
| $P_{GAE}$ | Probability Of Go-Around Catastrophe With No ILM |
| $P_{ELI}$ | Probability Of Emergency Landing Catastrophy With ILM |
| $P_{GAI}$ | Probability Of Go-Around Catastrophe With ILM |
| $P_{SBE}$ | Probability Of Catastrophe Using Strategy B With No ILM |
| $P_{SBI}$ | Probability Of Catastrophe Using Strategy B With ILM |
| $P_{MLE}$ | Probability Of Manual Landing Catastrophe With No ILM |
| $P_{MLI}$ | Probability Of Manual Landing Catastrophe With ILM |
| $P_{MAE}$ | Probability Of Missed Alarm - Primary Monitors |
| $P_{MAI}$ | Probability Of Missed Alarm - ILM (Inherent Rate) |
| $P_{ILM}$ | Probability Of Missed Alarm Due to ILM Failure |
| $P_{MAS}$ | Probability of Missed Alarm Of ILM;<br>$P_{MAS} = P_{MAI} + P_{ILM}$ |

## Evaluation Of System Requirements

With the formulation of the eight possible strategy combinations presented in Table 12, it is now possible to address the questions posed at the beginning of this chapter. This is done by considering the typical ranges of numerical values for the parameter which make up the equations of Table 12. Specific example values are selected for these parameters, and they are used to compute the resulting probability of catastrophic accident $P_A$. Then, the strategy which gives best results can be selected. Also, necessary equipment performance requirements can be ascertained.

Consider the first question: On what basis can an ILM be justified? The answer to this question has two parts - (a) the strategies which use the ILM information (Options 2, 3, and 4 in Table 11) must provide better safety results than without the ILM (Option 1) and (b) the improvement in safety or landing performance must be economically justified. Only the former condition is considered here.

The answer to the second question - How is the strategy associated with use of the ILM affected? - can be partially answered by determining which strategy (A or B) discussed previously provides the better results. The answer to the third question - On what basis will possible conflicting system failure indications of the existing autoland monitors be reconciled with those of the ILM? - is based on which option of Table 11 using the ILM provides the better answer. The answer to the fourth question - What are the technical requirements of the ILM fault detection equipment? - is based on what are the upper limits to the ILM false alarm rate and missed alarm rate which will still provide an acceptable catastrophic accident rate.

The answer to the fifth question--What are the fault detection timing requirements?--is not directly answered in this chapter. The strategies A and B use the altitude parameters h*, $h_1$*, and $h_2$*. These altitude values are given assumed values in this section so that the eight combinations of Table 12 can be numerically evaluated. Later, the total recovery timing requirements are evaluated and the results are used to reset the values of h* or $h_1$* and $h_2$*. The system designer can use these new values to recompute the ILM equipment performance requirements based on the options presented in this chapter. In this way, the ILM system design is an iterative process.

In the following, the nominal values of exposure factors resulting from the strategies A and B are first determined. Then, nominal values for autoland and other equipment failure probabilities and ILM failure probabilities are selected. These values are used to evaluate the probability of catastrophic accident, $P_A$. The basic design rule is to determine numerical values of the unspecified parameters to ensure that a specified level of safety $P_A$ is achieved. For numerical example, the FAA certification requirement of $P_A \leq 10^{-7}$ catastrophic accidents per landing is used.

All calculations assume that the total exposure period is 250 seconds. During the start of this period, the aircraft is assumed to enter the landing area with the onboard autoland system and the ILM system in an armed state. The assumed nominal values for the exposure factors are summarized in Table 14. In general, these values are very much aircraft dependent; for example, the Boeing 737 can execute a go-around from 20 feet wheel height whereas a Boeing 747 cannot.

Table 15 shows the results of computing typical values of probabilities of a catastrophe due to manual takeover ($P_{SAE}$, $P_{SAI}$, $P_{SBE}$, and $P_{SBI}$) with Strategies A and B and with and without an

TABLE 14.-EXPOSURE FACTORS USED FOR NUMERICAL EXAMPLES

| PARAMETERS | A | B | COMMENTS |
|---|---|---|---|
| $T_{1gs}$ | 5 | 5 | Exposure Period For Emergency Landing Decision |
| $T_{2gs}$ | 245 | 10 | Exposure Period For Go-Around Decision |
| $T_{3gs}$ | - | 225 | Exposure Period For Manual Landing Decision |
| $\alpha 1$ | .020 | .02 | Exposure Factor - Emergency Landing |
| $\alpha 2$ | .98 | .08 | Exposure Factor - Go-Around |
| $\alpha 3$ | - | .9 | Exposure Factor - Manual Landing |

ILM. These results are for assumed values of the terms $P_{GAE}$, $P_{ELE}$, $P_{MLE}$, $P_{ELI}$, $P_{GAI}$, and $P_{MLI}$ and the exposure factors given in Table 14. To justify Strategy B using an ILM, it is required that the probability of catastrophe during manual landing using ILM guidance is less than that using autoland monitors alone; that is

$$P_{MLI} \leq P_{MLE} \tag{5}$$

Moreover, the probability of catastrophe while executing a manual landing using an ILM should be less than or equal to that for executing a go-around using an ILM; this is

$$P_{MLI} \leq P_{GAI} \tag{6}$$

Table 15 indicates that Strategy B is unacceptable under Category III conditions, without an ILM, due to the excessively large contribution to accident catastrophe in attempting a blind landing without guidance aids; this is an intuitively obvious result.

TABLE 15.-EFFECTIVE CATASTROPHIC PROBABILITIES FOR STRATEGY A AND B, WITH AND WITHOUT ILM FOLLOWING MANUAL TAKEOVER

| PROBABILITY | VALUE | SITUATION OF CATASTROPHE | |
|---|---|---|---|
| $P_{GAE}$ | $10^{-3}$ | Go-Around Using Primary Monitors | |
| $P_{ELE}$ | 0.9 | Emergency Landing Using Primary Monitors | |
| $P_{MLE}$ | $10^{-5}$ | Category I | Manual Landing Using Primary Monitors |
| | $10^{-3}$ | Category II | |
| | 1 | Category III | |
| $P_{ELI}$ | $10^{-2}$ | Emergency Landing Using ILM Monitors/ Guidance | |
| $P_{GAI}$ | $10^{-4}$ | Go-Around Using ILM Monitors/Guidance | |
| $P_{MLI}$ | $10^{-4}$ | Manual Landing Using ILM Monitors/ Guidance | |
| $P_{SAE}$ | $2 \times 10^{-2}$ | Strategy A, Using Primary Monitors | |
| $P_{SAI}$ | $3 \times 10^{-4}$ | Strategy A, Using ILM Monitors/Guidance | |
| $P_{SBE}$ | $1.2 \times 10^{-2}$ | Category I | Strategy B, Using Primary Monitors; Unacceptable for Category III Visibility |
| | $1.7 \times 10^{-2}$ | Category II | |
| | 0.9 | Category III | |
| $P_{SBI}$ | $3 \times 10^{-4}$ | Strategy B, Using ILM Monitors/Guidance | |

A necessary condition for justifying the incorporation of an ILM is that using the ILM decreases the probability of catastrophe for one of the strategies; that is either

$$P_{SAI} \leq P_{SAE} \qquad (7)$$

or

$$P_{SBI} \leq P_{SBE} \qquad (8)$$

Finally, for the systems with ILM's, a necessary condition for choosing Strategy B over Strategy A is that the corresponding catastrophe probability for the former be less than the latter; that is

$$P_{SBI} \leq P_{SAI} \qquad (9)$$

The evaluation and verification of conditions (4) - (8) is done by performing a covariance propagation analysis. The method is presented in Chapter V and Appendix B.

Now consider the probability of catastrophic accident as a function of the equipment used. Table 16 contains assumed nominal values of the probability terms required to compute the total catastrophic accident probability $P_A$. All fault rates are based on a 250 second exposure period. For Strategy A and initiation Option 1, Table 17 illustrates the effect of improving the primary equipment failure rate $P_{EF}$ using the values given in Tables 14 and 16. The safety specification of $10^{-7}$ cannot be met; the limiting factor is the missed alarm probability $P_{MAE}$. Table 18 shows the effect of improving the primary equipment monitor missed alarm rate $P_{MAE}$; here again the safety requirement of $10^{-7}$ cannot be met with an equipment failure rate of $10^{-4}$.

When using the baseline data from Table 16, consider the effect of varying the primary equipment monitor false alarm and missed alarm rates ($P_{FAE}$ and $P_{MAE}$) with and without the ILM when Strategy A is used. In Table 19, Case 1 illustrates (via numerical example) that system performance will indeed be enhanced by an ILM, provided the fault detection performance of the ILM ($P_{FAI}$ and $P_{MAI}$) can be implemented. Case 2 illustrates that incorporation of an ILM does not improve overall performance appreciably if the normal missed alarm rate is reduced to $10^{-4}$. Case 3 shows that incorporation of an ILM using takeover Option 2 is insufficient to meet the safety

TABLE 16. - NOMINAL VALUES OF PROBABILITY TERMS REQUIRED TO COMPUTE $P_A$

| PROBABILITY | NOMINAL VALUE | COMMENT |
|---|---|---|
| $P_{EF}$ | $10^{-4}$ | MTBF ∿ 700 Hours; Autoland/MLS (Primary) Equipment Failure |
| $P_{ILM}$ | $10^{-4}$ | MTBF ∿ 700 Hours; ILM Hardware Failure Rate |
| $P_{fual}$ | 0.9 | Automatic Landing Catastrophe With Failed Primary Equipment |
| $P_{nual}$ | $10^{-8}$ | Automatic Landing Catastrophe Under Normal Operations |
| $P_{FAE}$ | $10^{-4}$ | Primary Monitor False Alar (Nuisance Disconnect) |
| $P_{MAE}$ | $10^{-1}$ | Primary Monitor Missed Alarm (Undetected Failure) |
| $P_{FAI}$ | $10^{-4}$ | ILM Monitor False Alarm (Nuisance Disconnect) |
| $P_{MAI}$ | $10^{-3}$ | ILM Monitor Missed Alarm (Undetected Failure) |

requirements, although there is almost two orders of magnitude improvement in $P_A$ by using the ILM. Consequently, the other options in Table 11 were examined by repeating Case 3. The ILM performance measures $P_{FAI}$ and $P_{MAI}$ were adjusted to achieve $10^{-7}$ for $P_A$.

Cases 4 and 5 in Table 19 show the result of considering these options. For the numerical values chosen, Option 3 is acceptable. Here, stringent requirements are placed on the ILM performance. Option 4 is preferred because the ILM false alarm and missed alarm rates required are more easily implemented in hardware than those required for Option 3.

TABLE 17. - EFFECT OF IMPROVING PRIMARY EQUIPMENT FAILURE RATE $P_{EF}$ ON PROBABILITY OF CATASTROPHE ACCIDENT $P_A$

| $P_E$ | $P_A$ | SAFETY LIMITING FACTORS |
|---|---|---|
| $10^{-4}$ | $1.2 \times 10^{-5}$ | $P_{EF}$ |
| $10^{-5}$ | $3 \times 10^{-6}$ | $P_{EF}$, $P_{MAE}$ |
| $10^{-6}$ | $2 \times 10^{-6}$ | $P_{MAE}$ |

TABLE 18. - EFFECT OF IMPROVING AUTOLAND MONITOR MISSED ALARM RATE $P_{MAE}$ ON $P_A$

| $P_{MAE}$ | $P_A$ | SAFETY LIMITING FACTORS |
|---|---|---|
| $10^{-1}$ | $1.2 \times 10^{-5}$ | $P_{MAE}$ |
| $10^{-2}$ | $4.9 \times 10^{-6}$ | $P_{MAE}$, |
| $10^{-3}$ | $4.1 \times 10^{-6}$ | $P_{MAE}$, $P_{EF}$ |

TABLE 19. - RESULTS OF CATASTROPHIC ACCIDENT PROBABILITY COMPUTATIONS

| CASE | ASSUMED VALUES | | | | $P_A$ FOR OPTION 1 | $P_A$ FOR ILM | |
|---|---|---|---|---|---|---|---|
| | $P_{FAE}$ | $P_{MAE}$ | $P_{FAI}$ | $P_{MAI}$ | | OPTION | VALUE |
| 1 | $10^{-4}$ | $10^{-1}$ | $10^{-4}$ | $10^{-3}$ | $1.2 \times 10^{-5}$ | 2 | $10^{-7}$ |
| 2 | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | $10^{-2}$ | $4 \times 10^{-6}$ | 2 | $10^{-7}$ |
| 3 | $10^{-3}$ | $10^{-3}$ | $10^{-4}$ | $10^{-2}$ | $2.2 \times 10^{-5}$ | 2 | $3.7 \times 10^{-7}$ |
| 4 | $10^{-3}$ | $10^{-3}$ | $3 \times 10^{-4}$ | $2 \times 10^{-4}$ | $2.2 \times 10^{-5}$ | 3 | $\sim 10^{-7}$ |
| 5 | $10^{-3}$ | $10^{-3}$ | $10^{-4}$ | $10^{-4}$ | $2.2 \times 10^{-5}$ | 4 | $\sim 10^{-7}$ |

A similar comparitive analysis of the various cases listed in Table 19 can be performed for Strategy B. The main point to be made by the above examples is that the answers to questions raised at the beginning of the chapter are very much system dependent.

## Summary

The method of providing overall system safety during the design of all advanced avionic systems with autoland and ILM (particularly under low visibility conditions) is presented in this chapter. This is done in the context of primary monitor and independent landing monitor design.

The basic accident probability equation is used to generate performance specifications for fault detection, discrimination, and recovery. The key parameters governing the fault detection/discrimination portion of the system are the false alarm rates, $P_{FAE}/P_{FAI}$ (nuisance disconnect), missed alarm rates, $P_{MAE}/P_{MAI}$ (undetected failure), and equipment failure rates ($P_{EF}/P_{ILM}$). Additional factors include the ILM input measurement sampling rate and absolute maximum time to detect and discriminate. The key parameters governing fault recovery performance are the probabilities of emergency landing failure ($P_{ELE}/P_{ELI}$), probability of go-around failure ($P_{GAE}/P_{GAI}$) and probability of manual landing failure ($P_{MLE}/P_{MLI}$). The fundamental basis for the justification of an ILM in an autoland system is seen to be a reduction in the probability of catastrophic accident while executing a landing or go-around. This basis also led to a procedure to resolve conflict between primary autoland and ILM monitors.

The system safety equation governs the performance tradeoffs in the equipment reliability, false alarm and missed alarm rates of the primary monitors and the ILM. Moreover, it also governs the required level of safety while executing a go-around or a landing decision.

# IV. FAULT DETECTION AND DISCRIMINATION

The allocation of total accident probability to meet safety requirements is performed in Chapter IV. The relationship between the system safety equation (4) and the performance specification for the fault detection and discrimination subsystem is illustrated in Figure 1. The specification is made in terms of the allowable false alarm rates, $P_{FAE}/P_{FAI}$ (nuisance disconnect), missed alarm rates, $P_{MAE}/P_{MAI}$ (undetected failure), and the inherent equipment failure rates $(P_{EF}/P_{ILM})$. Promising ILM software implementations incorporating fault detection and discrimination algorithms are now evaluated with reference to this specification, to ensure that the resulting avionics system meets the allowable accident probability. Thus, to select a specific scheme, the following points are addressed:

1. Is it possible to achieve the false alarm and missed and alarm rate performance required by the ILM?
2. Does the hardware implementation technology allow the desired equipment failure rates to be met?
3. How many measurement samples of a state are required to determine that a fault has occurred?
4. How accurate must each state be measured by the ILM?
5. How can the ILM be used to discriminate between the types of system faults?
6. How much will the error state build up before the ILM detects that the fault occurred?

This chapter begins by summarizing the main premises, arising from operational factors, on which the ILM hardware implementation and algorithm design are based. This is followed by modeling of the representative nature and magnitude of faults to be detected and discriminated. Then, two practical fault detection algorithms are presented together with the associated assumptions and computer simulation results. Subsequently, the philosophy of fault discrimination, taking into account operational constraints, is discussed. The sensors required--to measure particular aircraft states, to implement the fault detection and discrimination scheme--represent a significant portion of the ILM information requirements. Finally, the areas of required further work are summarized.

## Main Premises and Fault Models

The premises used in the ILM fault detection monitor design are as follows: (1) minimize the interconnection to the primary autoland system (e.g., sensors, servos, signal levels, etc.), (2) provide various levels of pilot involvement in the performance assessment, and (3) perform the assessment in terms of the present rather than the future (or predicted) position. Premise (1) allows avoiding the hardware problems of primary system reliability reduction, due to additional interconnections, and the consequent reduction in system safety. Premise (2) provides that the output of the ILM not be limited to simply a go/no go indication. Rather, it provides the option of a display format to enable the pilot to assess continually changes in performance and to develop a confidence for ILM generated commands over a period of usage. Premise (3) acknowledges the complex nature of making a prediction regarding future events, in the presence of nonstationary wind disturbances, on an aircraft possibly flying a curved decelerating flight path. Consequently, the failure detection algorithms only assess whether the current "state" is "abnormal".

Prior to discussion of fault detection and discrimination techniques, it is necessary to delineate the nature and magnitude of the faults under consideration.

Conventional autoland designers perform a laborious failure modes and effects analysis (FMEA) [18] to design the autoland hardware monitors. The two basic monitoring techniques are comparison and on-line monitoring [20]. Comparison monitoring is performed by comparing the outputs of two identical systems, and on-line monitoring is performed by measuring key signal parameters as a function of time (e.g., voltage amplitude and phase). The iterative design process of FMEA is conducted by analyzing the effect of faults (in terms of signal characteristics) at different points in a subsystem and then designing the minimum cost monitor to detect the fault before its effects become unacceptably large. Often this is a trial and error process; at each step in this iterative process, the fault monitor has to be moved electrically closer to the point in the subsystem where the fault is likely to occur. Ultimately, the monitor performance is improved until the fault detection specification for the overall avionics system can be met. The resulting design is highly aircraft/avionics system dependent and must be reworked for each new aircraft design.

On the positive side, usage of autoland system hardware monitors results in minimum time-to-detect any failure that is considered to be hazardous to normal flight operation and "not highly improbable." Indeed, the Federal Air Regulations (FAR's) require onboard indication of the operational status of all important systems and sensors. Specifically, the FAR's require that the crew be informed visually and orally of an autopilot malfunction or disconnection and the current autoland redundancy level. As noted previously, the MLS system, as currently planned, also has hardware monitors to inform the pilot and crew of malfunction and redundancy level. In general, the time-to-detect faults for the MLS and autoland hardware monitors is on the order of one second.

The purpose of the ILM fault detection subsystem is to (a) detect an "abnormal" condition, and (b) discriminate between the possible "failures". Due to the operational premise (1), stated previously, the ILM monitors must detect a failure by observing only the failure's effect on the aircraft state. Consequently, one can expect the ILM time-to-detect to be longer than that of a well-designed hardware monitor.

The possible system faults that the ILM can detect can be categorized into (a) autoland (e.g., guidance computers, autopilot), (b) MLS, (c) "out-of-design envelope" wind, and (d) ILM system malfunctions. Since minimal interconnection to the primary system is proposed, the failures are detected by measuring perturbations to the nominal aircraft trajectory (e.g., $\theta$, $\phi$, $\psi$, $x$, $y$, $z$, $\alpha$, $\beta$, $p$, $q$, $r$) with independent ILM sensors.

It is not necessary at this point to model explicitly the exact aircraft dynamics which results from a systems fault. The state perturbations because of a fault can be assumed to change either as a step or a ramp. For example, a fault causing the aircraft to roll would produce a ramp output from a vertical gyro and a step output from a roll rate gyro. Also, certain MLS beam noise or wind conditions could cause step or ramp changes in the measurement sensor output covariance. Therefore, the fault detection schemes can be based on measuring the changes in the mean and variance of each measurement sensor's output.

The measurement data have a certain amount of normal noise. This noise is surpressed by having a threshold which the state error must exceed before it can be considered "abnormal".

The fault detection system analysis considered potential faults in terms of their effect on the aircraft state. The typical range of state error buildup rates chosen for this study are presented in Table 20, for roll, sideslip, pitch and heading. Note that hardover faults are easier to detect (i.e., small time-to-detect) and more difficult to correct. On the other hand, slowovers are difficult to detect (i.e., long time-to-detect) and somewhat easier to correct. The principal difficulties in detecting slowovers is due to the effect of slowovers being masked by sensor noise and the nominal state activity due to the external environment (i.e., turbulance). Table 21 gives the assumed nominal noise activity on a one sigma basis, in the roll, pitch and heading states due to the external environment, normal autoland control activity and normal MLS beam noise/bends.

## Fault Detection Algorithms

Prior to describing the specific detection scheme proposed and the associated simulation results, some comments regarding the

TABLE 20.-TYPICAL STATE PERTURBATIONS CAUSED BY SYSTEM FAULTS

| TYPE OF FAILURE | ROLL RATE<br>$\dot{\phi}$ (°/SEC) | SIDESLIP RATE<br>$\dot{\beta}$ (°/SEC) | PITCH RATE<br>$\dot{\theta}$ (°/SEC) | HEADING RATE<br>$\dot{\psi}$ (°/SEC) |
|---|---|---|---|---|
| HARDOVER | 5 | 7.5 | 2 | 2 |
| SLOWOVER | 0.01 | 0.02 | -0.01 (NOSEDOWN)<br>+0.1 (NOSEUP) | 0.1 |

TABLE 21.-ASSUMED NOMINAL STATE ACTIVITY DUE TO ENVIRONMENTAL NOISE (1$\sigma$)

| STATE | ROLL | SIDESLIP | PITCH | HEADING |
|---|---|---|---|---|
| NOMINAL | 0.32° | 0.32° | 0.65° | 0.32° |

methodology are in order. Recall from the previous chapter that the basic pilot action for Strategy A, on failure detection, is to initiate a go-around. Because of time criticality of the approach, the precise cause of the failure is of secondary importance. Thus, the fault detection process receives major emphasis at this point.

Basic assumptions in the fault detection scheme are that (1) the sequence of samples obtained from the sensors on each state arise from a normal Gaussian distribution and (2) the samples are uncorrelated. These assumptions are made because no results exist in the literature without these assumptions at this time. The former assumption of "normality" does not have as significant an impact as the latter. From the physics of the problem it is clear that sequential samples of aircraft state measurements are in fact correlated, but these can be made uncorrelated by a whitening filter [21] or an ARMA (auto-regressive moving average -- minimal order discrete differential equations modeling the input/output behavior) model [21]. Both these approaches require the availability of flight test/simulator data, and additional computation time is required for the whitening process. In any case, the robustness of any statistical sample testing algorithm to test assumptions must be determined by simulation methods.

Difficulties arise in detecting the faults from the measured state perturbations because: (1) the allowable time to detect (from a recovery point-of-view) for hard failures is limited to some maximum time T and (2) the effect of slowovers are masked by the effect of the normal disturbances indicated in Table 21. An increase in the wind disturbance magnitude or a performance degradation in the MLS or autoland system is reflected by an increase in the variance of the system state statistics. On the other hand, a hardover or slowover failure results in a change in the mean values of some or all of the states.

In summary, the statistical tests should detect changes in mean and/or variance from the "nominal", within T seconds, using a fixed sampling rate. Also to meet ILM performance constraints, the detection logic should have a fixed false alarm (nuisance disconnect) rate $P_{FAI}$ and a fixed missed alarm (undetected failure) rate of $P_{MAI}$. Based on industry data and the calculations of the previous chapter, a typical set of numerical values of these parameters is presented in Table 22.

TABLE 22.- FAULT DETECTION ALGORITHM PERFORMANCE SPECIFICATION

| T(SEC) | K(SAMPLES/SEC) | $P_{FAI}(\eta)$ | $P_{MAI}(\zeta)$ |
|---|---|---|---|
| 2 | 10 | $10^{-4}$ | $10^{-3}$ |

A number of statistical tests can be used, depending on the hypothesis being tested [22-25]. The applicable tests to detect mean and variance changes, are summarized in Table 23. In the leftmost column, the hypotheses being tested are tabulated; these fall into two main categories -- mean changes and variance changes. For each of these categories, there exists the univariate sample case and the multivariate sample case.

As noted in the references, a number of unsolved problems remain in the area of statistical testing. One particular case is the generation of fault detection operating characteristics for the t test. Current literature indicates that these characteristics must be determined by extensive Monte Carlo computer simulation.

Let $\{x_i\}_{i=1}^{n}$ be a sample from a normal distribution with constant mean $\mu_o$ and variance $\sigma_0^2$. To test whether a given sample $\{x_i\}$ satisfies the null hypothesis $(\sigma^2 = \sigma_o^2)$ or the alternate $(\sigma^2 \neq \sigma_0^2)$ one can perform either a likelihood ratio test [22] or a chi-square $(\chi^2)$ test. Even under the assumptions of normality and independent samples, the likelihood ratio test is a complex function of the sample variance. Analytical or empirical results on the distribution of the likelihood ratio tests, necessary to compute test thresholds, are not available in literature. Therefore, in practice, a chi-square $(\chi^2)$ test for the null hypothesis (denoted by $\mu_0$: $\sigma = \sigma_0^2$) is used. This test is also used here, for detecting univariate variance changes as documented in Table 23.

TABLE 23.-APPLICABLE PARAMETRIC STATISTICAL TESTS

| HYPOTHESES | UNIVARIATE | | MULTIVARIATE (ONE-SIDED NOT APPLICABLE) | |
|---|---|---|---|---|
| MEAN | σ KNOWN | σ UNKNOWN | σ KNOWN | σ UNKNOWN |
| $H_o: \mu = \mu_o$<br>$H_1: \mu \neq \mu_o$ | Z TEST:<br>$Z_o = \frac{1}{2} \log \frac{1+r}{1-r}$<br>r: CORRELATION COEFFICIENT (BI-VARIATE) | t TEST:<br>$t_o = \frac{(\overline{X}-\mu_o)}{S}\sqrt{n}$<br>ROBUST TO NORMALITY ASSUMPTION<br>$\overline{X} = \frac{1}{n} \sum_{i=1}^{n} X_i$ | $\chi^2$ TEST<br>(VECTOR CASE) | $T^2$ TEST:<br>$T^2 = N(\overline{X}-\mu_o)^T, S^{-1}(\overline{X}-\mu_o)$<br>$T^2 = (N-1)\ (\lambda_o^{-2/N} - 1)$<br>S = COVARIANCE MATRIX<br>$\lambda_o$ = CONFIDENCE LEVEL SETTING |
| VARIANCE<br>$H_o: \sigma^2=\sigma_o^2$<br>$H_1: \sigma^2\neq\sigma_o^2$<br>$\sigma^2>\sigma_o^2$ | MAXIMUM LIKELIHOOD TEST<br>LARGE SAMPLE APPROXIMATION: $\chi^2$<br>μ KNOWN/UNKNOWN<br>$\chi_o^2 = \frac{(n-1)S^2}{\sigma_o^2}\ ; S^2=\frac{1}{n-1} \sum_{i=1}^{n} (X_i-\overline{X})^2$<br>NOT ROBUST TO NORMALITY ASSUMPTION | | MAXIMUM LIKELIHOOD TEST<br>LARGE SAMPLE APPROXIMATION: $T^2$<br>μ KNOWN/UNKNOWN | |

To test the hypothesis of whether the mean $\mu$ is equal to some constant $\mu_0$ (denoted by $H_0$: $\mu = \mu_0$) or it is not (denoted by $H_1$: $\mu \neq \mu_0$), the student's t test is used when the variance $\sigma^2$ is unknown. Unlike the $\chi^2$ test, the t test (see Table 23) is robust (i.e., insensitive to moderate deviations from the assumption of normality) when the sample is random. But unlike the $\chi^2$ test, analytic expressions or tabulated results are not available to determine the test threshold setting to achieve a prespecified false alarm rate ($\eta$) and missed alarm rate ($\zeta$).

For the $\chi^2$ test, Figure 13 presents the variance ratio that can be detected as a function of sample size (n), false alarm rate ($\eta$) and missed alarm rate ($\xi$) [24]. These curves were obtained by evaluating analytic expressions of the $\chi^2$ test using numeric values of the false alarm ($\eta$) and missed alarm ($\xi$) rates. Based on requirements defined in Table 22, it was determined that to detect an "abnormal" condition in a given signal, the change in variable from "normal" ($\sigma_0{}^2$) to "abnormal" ($\sigma_m{}^2$) must be 9.55. The corresponding null and alternative hypotheses for the $\chi^2$ test are shown in Table 24 for the roll, pitch, and heading axes.

The proper threshold setting and the corresponding mean change required to identify an abnormal signal in the t test had to be determined by computer simulation. This is as yet an analytically unsolved problem.

TABLE 24.-THE NULL AND ALTERNATE HYPOTHESIS FOR THE $\chi^2$ TEST

| STATE | ROLL | PITCH | HEADING | COMMENTS |
|---|---|---|---|---|
| NOMINAL | 0.32° | 0.65° | 0.32° | $H_0$: NULL HYPOTHESIS |
| DETECTABLE | 1.0° | 2.0° | 1.0° | $H_A$: ALTERNATIVE HYPOTHESIS |

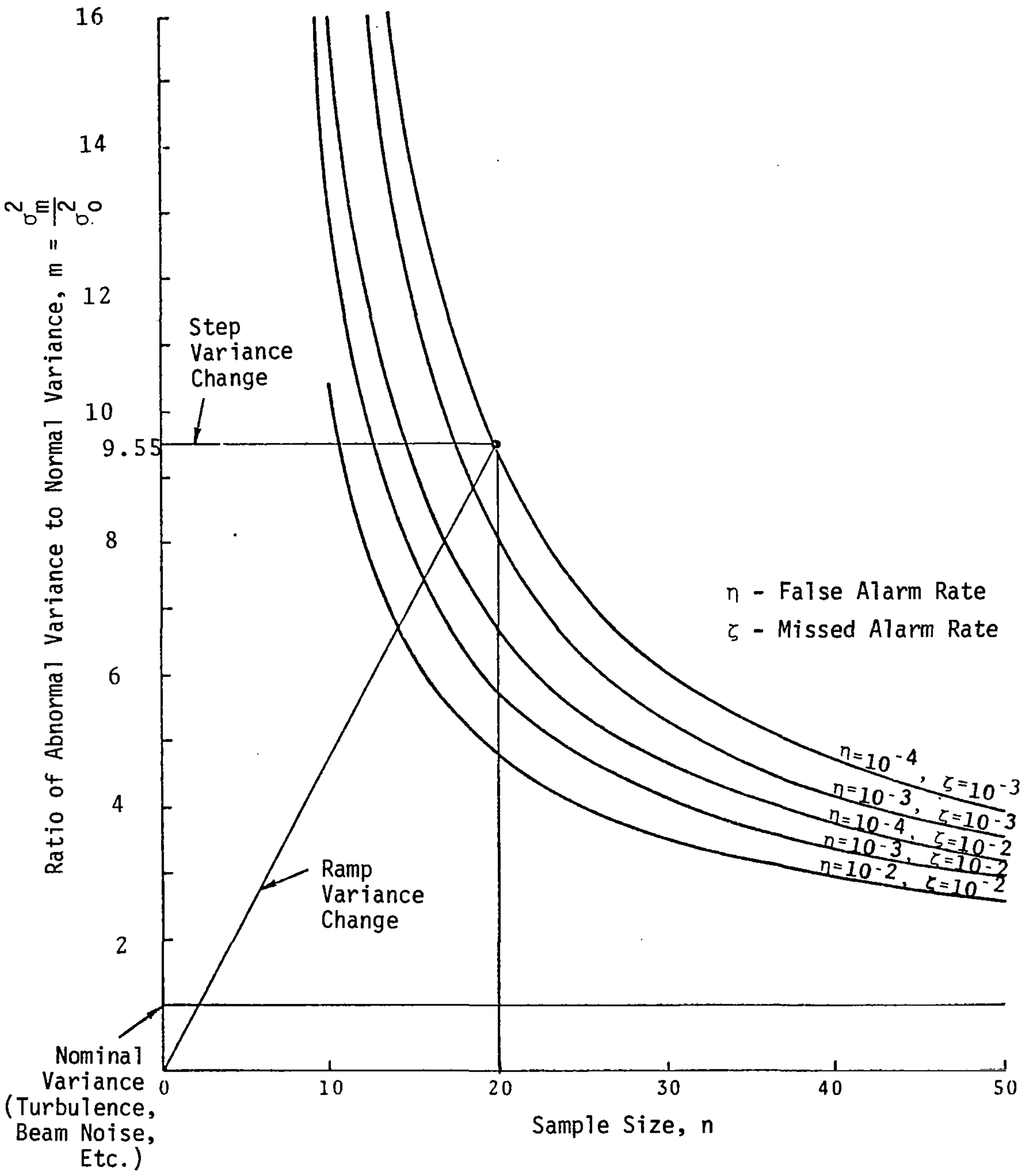


FIGURE 13.-DETECTION CHARACTERISTICS OF THE $\chi^2$ TEST

For the present study, computer simulations were performed to validate the effectiveness of the t test and $\chi^2$ test, for the univariate case, using step and ramp changes, in the mean and variance of the measured state. The performance of the tests was evaluated using 10,000 runs of 50 samples each. To obtain more statistically correct results would require more runs. This was not done to minimize computation costs. In each case, step and ramp changes to the measured state, because of faults, were introduced after 20 samples. The form of these changes are shown in Figures 14a and 14b, respectively.

The corresponding simulation results for a mean change and a variance change are shown in Figure 15a and 15b, respectively. These figures indicate that, as expected, step faults are easier to detect than ramp faults. Simulation results are summarized in Table 25. It can be seen that $\chi^2$ test is not robust to changes in the mean. In other words the $\chi^2$ test, used to detect changes, has a high false alarm ($\eta$) rate for changes in the mean. On the other hand, the t test, used to detect mean changes, does not cause a false alarm when there is a change in variance. Thus, the t test is robust to variance changes.

The robust feature of the t test can be used to alleviate the shortcoming of the $\chi^2$ test, when both tests are used simultaneously. A simple hardware implementation of the required logic is shown in Figure 16. Essentially the shortcoming of the $\chi^2$ test is overcome by declaring a change in variance only if the t test does not flag a change but the $\chi^2$ test does.

A significant amount of additional work needs to be performed on detection algorithm methods to answer a number of pertinent problems:

1. Determination of threshold setting for the t test as a function of the samples size (n), false alarm rate ($\eta$) and missed alarm rate ($\zeta$).

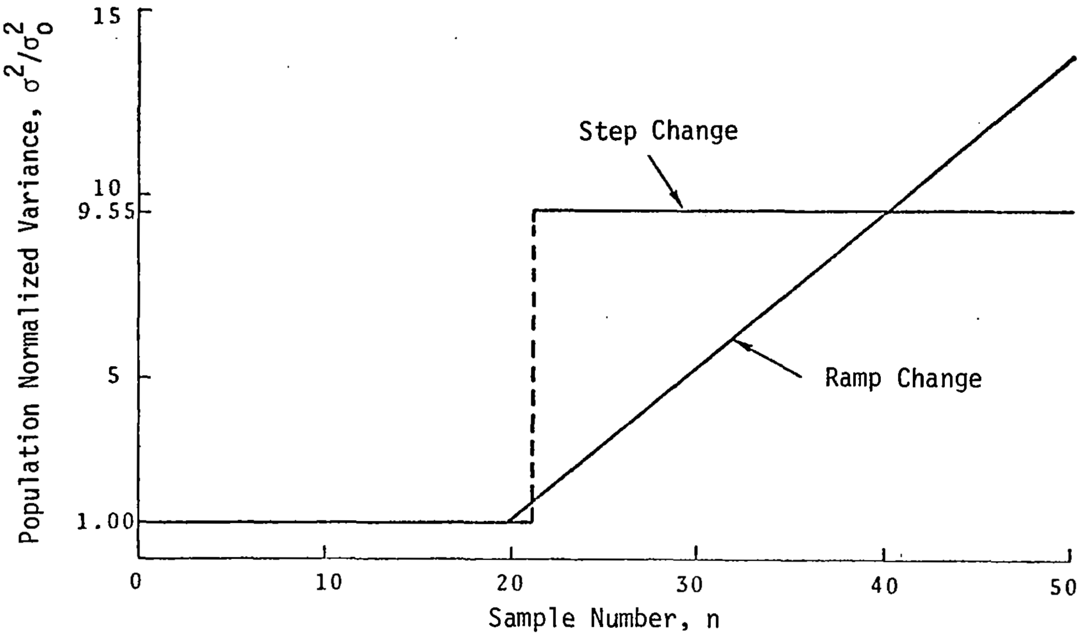


FIGURE 14 a.-STEP AND RAMP FAULT IN VARIANCE

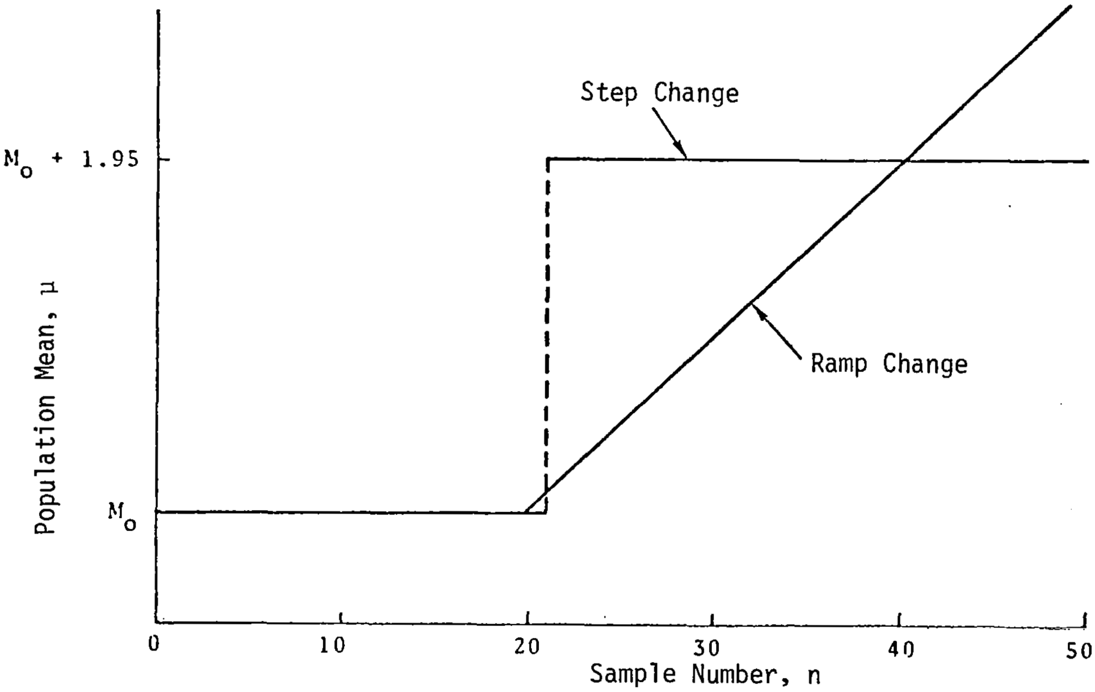


FIGURE 14b-STEP AND RAMP FAULT IN MEAN

2. Methodology for threshold setting and false alarm/missed alarm rate computation for state errors with ramp growth characteristics.
3. Extension of (1) and (2) to the vector test (i.e., the $T^2$ and $\chi^2$ tests).

## Fault Discrimination

In examining the results of the previous chapter, one notes that a primary requirement is to detect the presence of a fault.

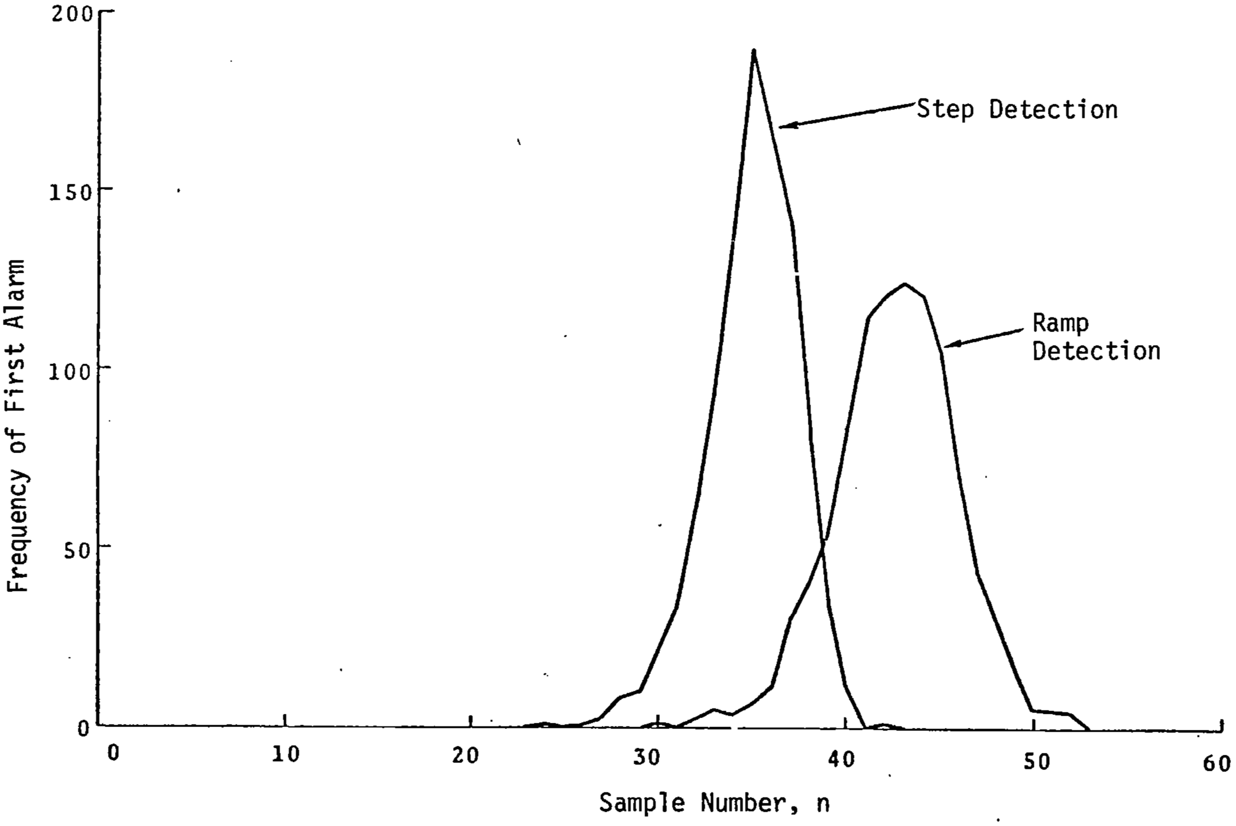


FIGURE 15a.- FREQUENCY DISTRIBUTION OF FAULT DETECTION FOR MEAN CHANGE

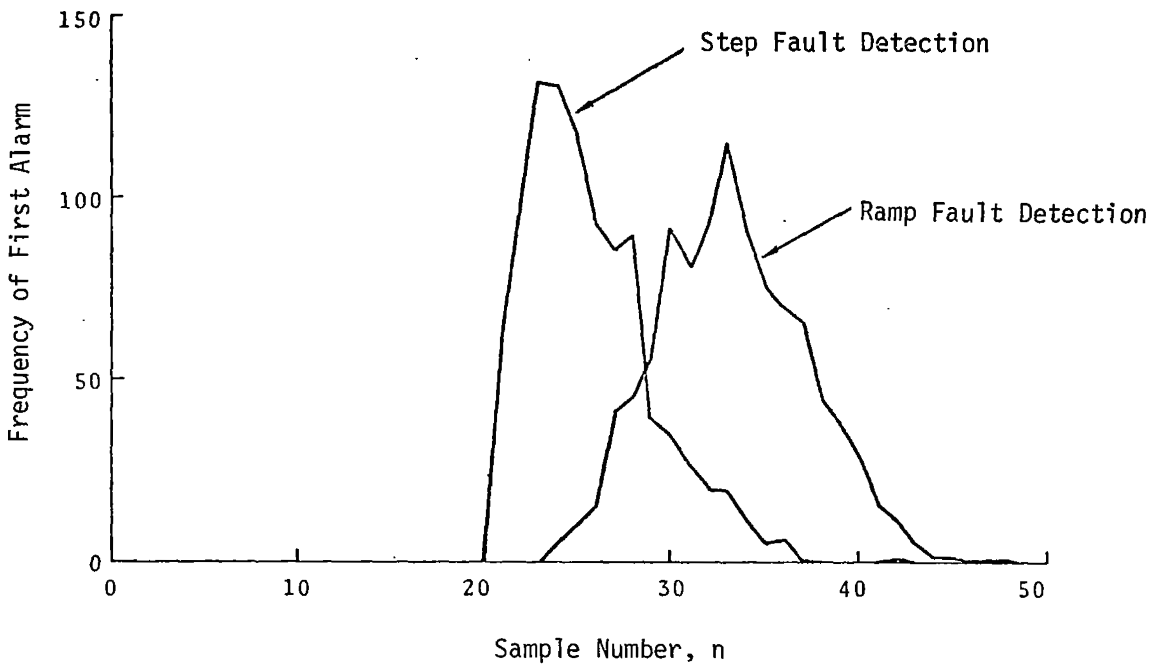


FIGURE 15b.-FREQUENCY DISTRIBUTION OF FAULT DETECTION FOR VARIANCE CHANGE

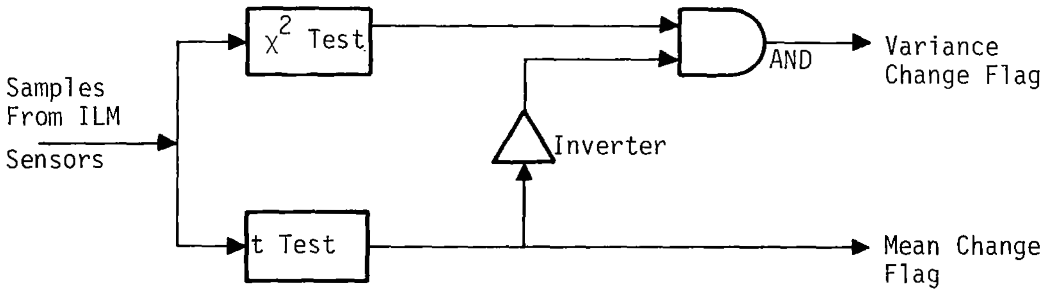


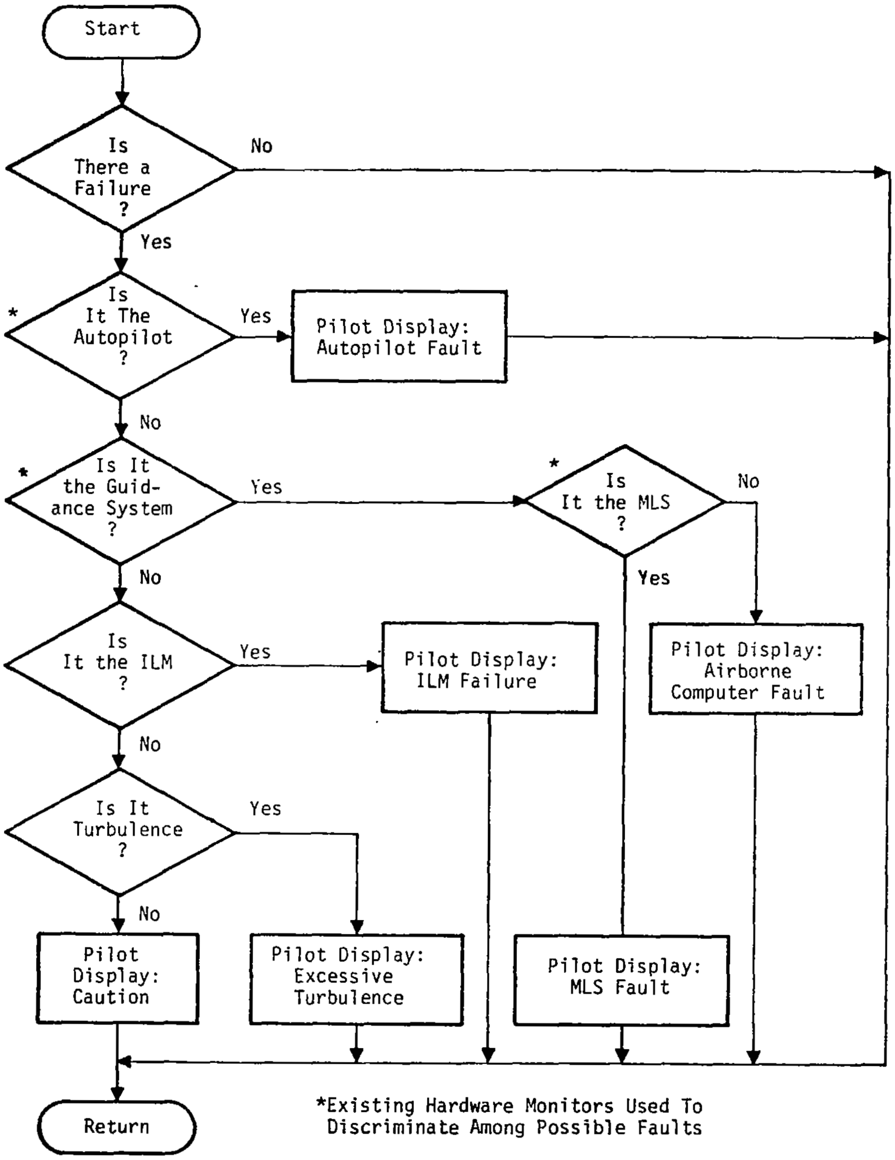
FIGURE 16.-PROPOSED DETECTION LOGIC TO PROVIDE ROBUSTNESS IN $\chi^2$ TEST

TABLE 25.- COMPUTER SIMULATION RESULTS FOR THE $\chi^2$ AND t TEST

| INPUT CHANGE CHARACTERISTIC | | FALSE ALARM RATE ($\eta$) | | MISSED ALARM RATE (S) | | COMMENTS |
|---|---|---|---|---|---|---|
| TYPE | ELEMENT | $\chi^2$ | t | $\chi^2$ | t | |
| Step | Mean | 0.366 (High False Alarm Rate) | $10^{-4}$ | -- | $10^{-3}$ | Excessive $\eta$ for Mean Change, Using $\chi^2$ |
| | Variance | $10^{-4}$ | 0 | $10^{-3}$ | -- | Increased Turbulence/Beam/Noise/ AP Degradation |
| Ramp | Mean | 0.003 | $10^{-4}$ | -- | $10^{-3}$ | Excessive $\eta$ for Mean Change, Using $\chi^2$ |
| | Variance | $10^{-4}$ | $3 \times 10^{-4}$ (Small Alarm Missed) | $10^{-3}$ | -- | Increased Turbulence/Beam/Noise/ AP Degradation |

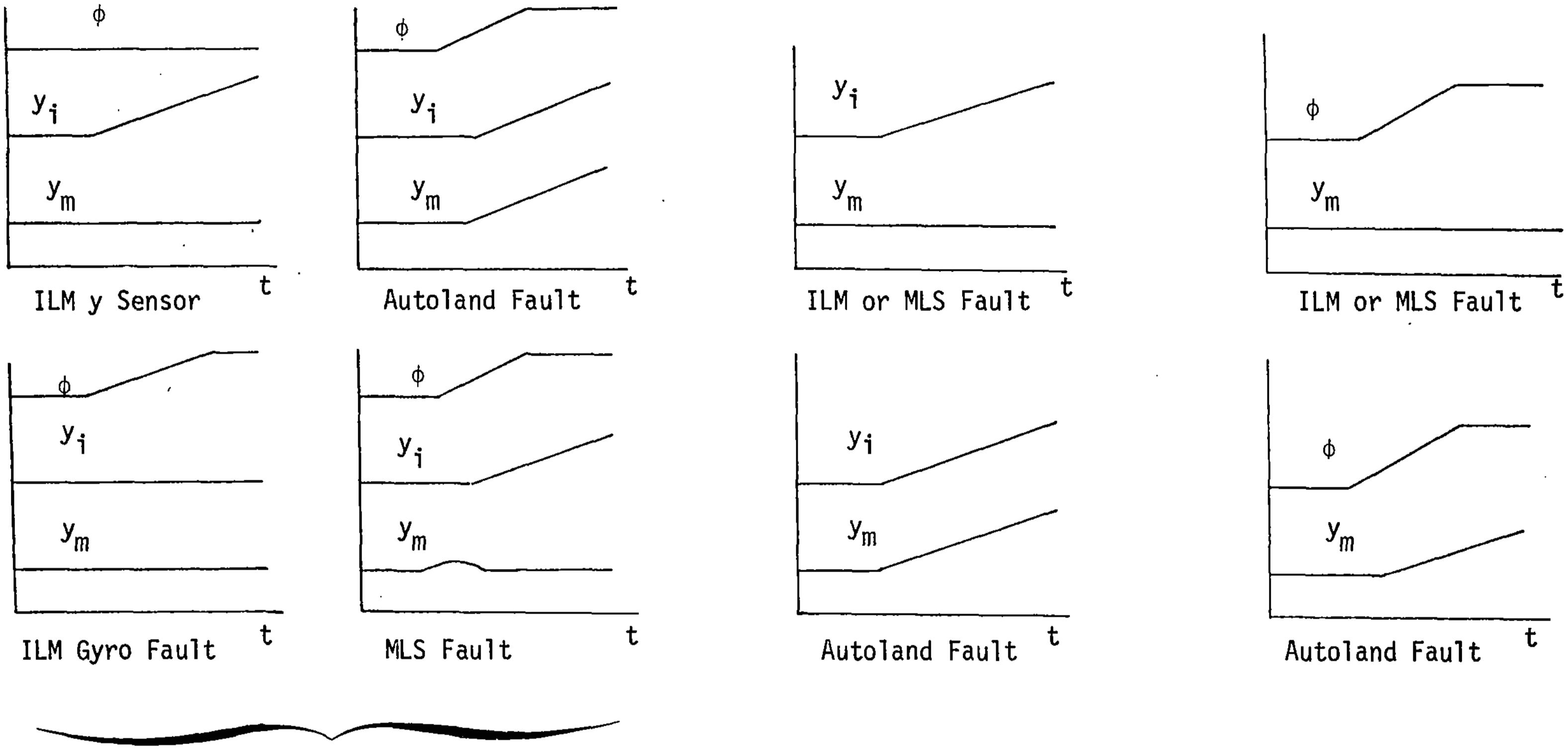
To discriminate among the various fault categories, one procedure is to check sequentially all the autoland/MLS hardware monitor flags and to identify the fault source by a process of elimination. One posible discrimination flow chart, to accomplish this, is presented in Figure 17. Basically, the priority for performing the sequential discrimination is to perform the validity checks first on the subsystems (e.g., autopilot) whose failures lead to the greatest hazard probability.

An alternative methodology for fault distrimination without the use of existing hardware monitors is to compare signals from independent sources for consistency using simple system dynamic mdoels. For example, a fault causing a roll angle must eventually show up as a lateral displacement. Assuming that the ILM position and attitude information is independent, Figure 18 shows sketches of the measurement traces due to faults causing lateral deviations in the error state. Shown are typical amplitudes of ILM gyro measured roll angle ($\phi$), ILM y-sensor measured lateral position ($y_i$), and MLS measured lateral position ($y_m$). As can be seen in Figure 18a, if both ILM gyro and y-sensor data are available, autoland, MLS, and ILM faults can be distinguished. With only y-sensor (Figure 18b) or gyro (Figure 18c) data, an autoland failure can be distinguished from an ILM or MLS fault, but the ILM and MLS faults can't be differentiated directly. However, if the presence of a fault is the only information required, the two sources are adequate. Similarly, a single source (either y-sensor or gyro) could be used to determine that a fault of some sort is present (ILM, MLS, or autoland).



*Existing Hardware Monitors Used To Discriminate Among Possible Faults

FIGURE 17.-SEQUENTIAL DISCRIMINATION TEST FLOW CHART



(a) Three Independent Signals

(b) No ILM Gyro

(c) No ILM y Sensor

FIGURE 18.- LATERAL SIGNAL TRACES INDICATING ILM, MLS, OR AUTOLAND FAULT OCCURRENCE; (a) ILM ASSUMED TO HAVE BOTH POSITION ($y_i$) AND ATTITUDE ($\phi$) INFORMATION; (b) ILM HAS POSITION INFORMATION ONLY; (c) ILM HAS ATTITUDE INFORMATION ONLY.

# V. FAULT RECOVERY PERFORMANCE

The fault detection algorithms described in the previous chapter provide the pilot with an alarm advising him of the existance of a fault. The results of the safety analysis can be used to recommend an appropriate recovery decision (i.e., manual takeover to land or go-around). However, the validity of the choice is related to the time required to recover from the error state induced by the fault. At the point of fault detection, due to the statistical nature of the fault occurrence and detection process, the system state x is described by a mean deviation from nominal, $\overline{x}$, and a covariance, P, characterizing dispersions about this mean in a probabilistic sense. As noted in Fig. 1, specific fault recovery constraints, imposed by the safety analysis are defined in terms of the probabilities of emergency landing failure ($P_{ELE}/P_{ELI}$), probability of go-around failure ($P_{GAE}/P_{GAI}$) and probability of manual landing failure ($P_{MLE}/P_{MLI}$). To enable the pilot to recover from an upset and, subsequently guide the aircraft to a landing or go-around within these constraints, necessitates the incorporation of additional sensors and display parameters. The set of sensors and display parameters necessary to meet the above mentioned safety constraint, characterize the ILM information and display requirements.

The objective of this chapter is to present an evaluation of the performance of the pilot-aircraft-display system in recovery from an upset condition, based on the analysis described in Chapter IV. This performance of time-to-correct the fault, can be used to define quantitatively the altitudes which govern the recovery strategy. First, the technique of evaluating post-fault system performance (namely, covariance propagation) is presented in an outline form; a more detailed exposition is contained in Appendix B. Subsequently, simulation results for a particular set of numerical values corresponding to a linearized model of the terminally configured vehicle (B-737) are presented. These preliminary results allow an assessment to be made of the fault recovery performance as a function of initial state covariance, display accuracies, and pilot response characteristics.

## Fault Recovery Performance Assessment By Covariance Propagation

Two distinct techniques are available to evaluate post-fault system performance; these are the Monte Carlo analysis [15] and covariance propagation [21]. The former technique has been exclusively used by a number of commercial aircraft system developers to generate certification requirement compliance data for Category III autoland systems [15]. The latter technique has mainly been used in analytical studies.

The principal advantage of Monte Carlo methods over covariance propagation is that the results are more accurate. The Monte Carlo simulation allows the inclusion of all nonlinear details of the overall system being studied. On the other hand, the computation time for the Monte Carlo simulation can be excessive, particularly when the tails of the outcome probability distribution are to be evaluated. Moreoever, the time required to develop the program is quite substantial.

Because the present study focused on the development of a methodology for determining information and display requirements, the covariance propagation technique was selected to study recovery performance. Although the results are less accurate than those obtained by Monte Carlo analysis, this novel application of the technique does yield useful results pertinent to the complex, costly, and time-consuming process of advanced aircraft ILM design.

The application of the covariance propagation technique to evaluate recovery performance requires a linear small perturbation system model or sequence of models. These models define the aircraft-autoland-display-pilot system as it proceeds along the terminal area landing trajectory. Detailed analytical characterization of the system model and the covariance propagation technique is presented in Appendix B.

Figure 19 shows a system level block diagram for the manual control of the aircraft during a particular flight condition along the trajectory. The three essential subsystems in this diagram are the aircraft model, the display model, and the pilot model.

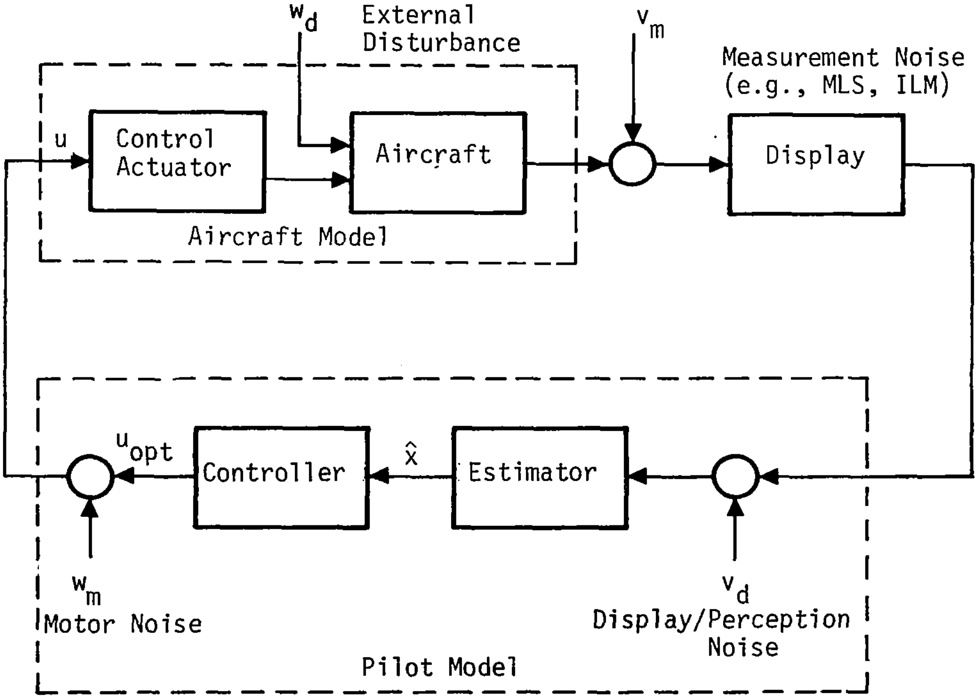


FIGURE 19.- MANUAL CONTROL SYSTEM BLOCK DIAGRAM

Note that the system model definition is in terms of perturbations about the nominal. The effects of sensor errors (e.g., MLS, ILM, altitude) are modelled by the noise variance $v_m$ introduced by them. Similarly, display noise is modelled by the noise variance $v_d$. The basic assumption in modelling the pilot is that he behaves as an optimal state estimator followed by a feedback controller to null out perturbations from the nominal [26,27]. To model the effects of pilot muscular motor noise in implementing these manually generated optimal control laws, a noise term $w_m$ is introduced. Finally, to model external gust-turbulence disturbances another noise term $w_d$ is used.

The state of the system at the point of fault detection is modelled by the mean state vector, $\bar{x}$, offset from the nominal (null) trajectory. A covariance matrix P represents the dispersion of the state about this mean, in a statistical sense. The closed loop aircraft-display-pilot feedback control system performance is obtained by numerically integrating the corresponding differential equation governing the propagation of the covariance matrix as a function of time. Typical covariance propagation results are graphically illustrated for the landing and go-around tasks, in Figures 20a and 20b, respectively, for the altitude state.

To determine whether the landing or go-around is "successful", the propagated covariance on a {(mean) ± k (sigma)} basis must be entirely within the appropriate state constraints (e.g., obstacle clearance, angle-of-attack limit). The probability of catastrophic failure due to a landing or go-around, as stated in the preceding error budget discussion and Appendix A, dictates the corresponding numerical value of k. The relationship between the parameter k and the failure probability is quantitatively presented in Appendix B.

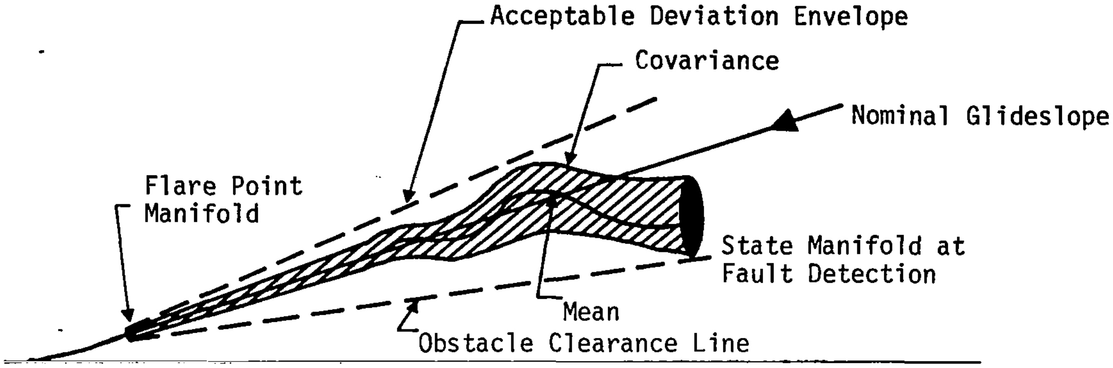


FIGURE 20a.-MANUAL LANDING TASK FAULT RECOVERY

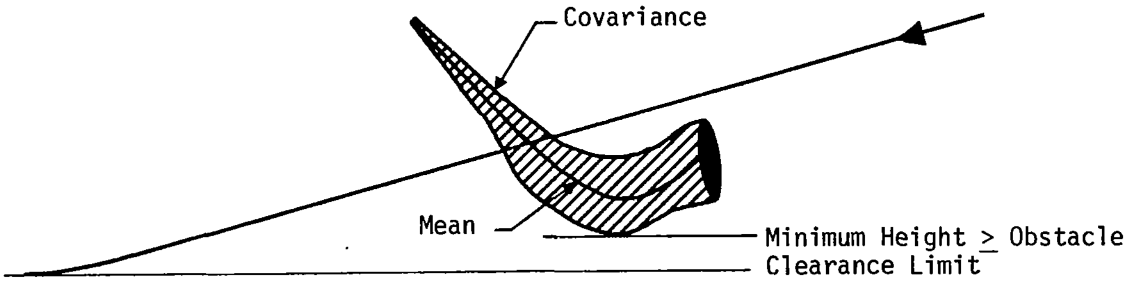


FIGURE 20b.-MANUAL GO-AROUND TASK FAULT RECOVERY

At each point along the approach trajectory, the error state covariance must be within the appropriate state constraints. If it is not, then it can be concluded that for the assumed initial state covariance and pilot model parameters, fault recovery at a sufficiently low level of catastrophe probability is not feasible.

The "time-to-correct", from an initial upset condition at fault detection, is evaluated in this fashion. A state covariance matrix characterizing the steady state covariance (due to external disturbance) when no faults are present is compared to that obtained from covariance propagation from the initial fault state. When the latter covariance is entirely within the former, the corresponding time-to-correct is obtained. Details on this recovery termination condition are given in Appendix B.

Besides evaluating probability of catastrophe and time-to-correct, covariance propagation allows convenient analysis of the sensitivity to the magnitude of sensor errors ($v_m$), display errors ($v_d$), external disturbances ($w_d$), and the pilot model parameters for the estimator and the controller. In the present study, partial results relating some of these factors were obtained. A substantial amount of further work, particularly with respect to pilot model parameter sensitivity, remains to be performed.

Two particular phases of flight, specifically the flare and go-around maneuvers, require further comments. Both these maneuvers involve non-linear system dynamics. The flare maneuver has a non-linear control sequence and non-linear ground effects on the aerodynamic coefficients. The go-around maneuver is nonlinear because of the limiting controls and abrupt change in flight conditions involved. Consequently, to obtain covariance propagation of reasonable fidelity to the true situation in these regimes, it is necessary to model these phases by a sequence of linear models rather than a single model. This requirement detracts from the principal features of covariance propagation, namely, ease of implementation and small computation time. In any case, the results of covariance propagation must be treated as a first approximation to advanced aircraft ILM design. These results must be validated by Monte Carlo analysis using the nonlinear equations of motion, ground-based cockpit simulation, and finally a prototype flight test. Nonetheless, covariance propagation does serve to provide approximations to the sensitivity of time-to-correct to system parameter variations. It also serves to determine which system parameters should be examined more closely in subsequent analysis and testing.

## Example Covariance Propagation Simulation Results

To determine the pilot recovery performance after fault detection, the longitudinal and lateral modes of the Terminally Configured Vehicle (TCV) were modeled by linearized sets of perturbation equations for the aircraft and an optimal control model for the pilot. Numerical data on these models are presented in Appendix B.

Starting with an initial state error covariance manifold ($\sigma_c$) and display error statistics ($\sigma_s$), the objective the the simulation was to determine the sensitivity of time-to-recover to changes in $\sigma_c$ and $\sigma_s$. This was done for both the longitudinal and lateral axes recovery decisions.

The baseline system was characterized by the set of numerical values in Table 26. These baseline standard deviations were varied as shown in Table 27. Based on the error budget requirements, the probability of catastrophic accident, during a go-around or landing decision, was constrained to be about $10^{-4}$ (1 accident per 10,000

TABLE 26.-COVARIANCE PROPAGATION BASELINE DISPLAY ERROR $(\sigma_s)$ AND INITIAL STATE ERROR $(\sigma_s)$ STANDARD DEVIATIONS

LONGITUDINAL ERRORS

ILM Display Error: $\sigma_s(\theta,u,\alpha,h,R_s)$ = { 1°, .52 m/s (1.7 Feet/s), 1°, .3 (1 foot), 1.5m (5 feet)}

Initial State Error: $\sigma_c(\theta,u,\alpha,h,R_s)$ = {2°, .52m/s (1.7 Feet/s), 2°, 3.05m (10 Feet), 6.1m (20 Feet)}

LATERAL ERRORS

ILM Display Error $\sigma_s(\phi,\psi,\beta,L)$ = {1°, 1°, 1°, 1.5m (5 Feet)}

Initial State Error: $\sigma_c(\phi,\psi,\beta, p,r,L)$= {1°, 1°, 1°, 1°/s, 1°/s, 7.6m (25 Feet)}

where

| | | | |
|---|---|---|---|
| $\theta$ | - Pitch angle | $\phi$ | - Roll angle |
| u | - Normalized velocity | $\psi$ | - Heading angle |
| $\alpha$ | - Angle-of attack | $\beta$ | - Sideslip angle |
| h | - Altitude | p | - Roll rate |
| $R_s$ | - Slant range | r | - Yaw rate |
| | | L | - Lateral displacement |

decisions). This corresponds approximately to the four sigma (4σ) covariance dispersion envelope as discussed in Appendix B. During each time step of the covariance propagation integration, this four sigma dispersion was constrained to lie within the appropriate aerodynamic and obstacle clearance constraints, shown in Table 28. The time-to-correct was the time required to satisfy the flare point window, given in Table 28.

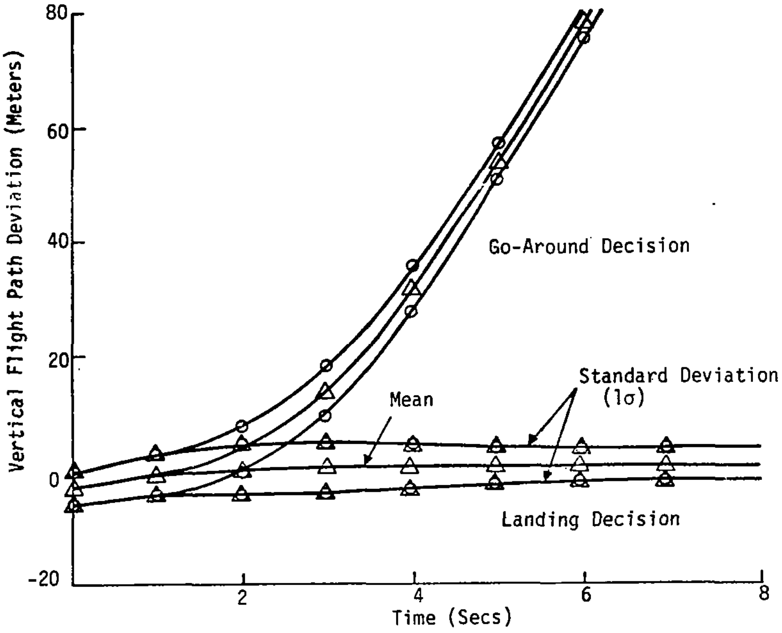
TABLE 27. - FAULT RECOVERY TIME-TO-RECOVER SENSITIVITY RESULTS VARIABLE ILM DISPLAY ERRORS AND AIRCRAFT STATE ERRORS (DUE TO FAULTS)

| AXIS | CASE | ILM DISPLAY | INITIAL STATE ERROR | LANDING ($4\sigma$) SEC | GO AROUND* ($4\sigma$) SEC | COMMENTS |
|---|---|---|---|---|---|---|
| LONGI-TUDINAL | 1 | $\sigma = \sigma_s$ | $\sigma = \sigma_c$ | 14 | 6.2 | Baseline |
| | 2 | $\sigma = 2\sigma_s$ | $\sigma = \sigma_c$ | 14 | 6.2 | Doubling Display Error |
| | 3 | $\sigma = \sigma_s$ | $\sigma = 2\sigma_c$ | 18 | 8.8 | Doubling Initial Covariance |
| | 4 | $\sigma = \sigma_s$ | $\sigma = \sigma_c/2$ | 12 | 4.0 | Halving Initial Covariance |
| | 5 | $\sigma = \sigma_s/2$ | $\sigma = \sigma_c/2$ | 12 | 4.0 | Halving Initial Covariance and Display Error |
| LATERAL | 6 | $\sigma = \sigma_s$ | $\sigma = \sigma_c$ | 18 | 10.2 | Baseline |
| | 7 | $\sigma = 2\sigma_s$ | $\sigma = \sigma_c$ | 18 | 10.2 | Doubling Display Error |
| | 8 | $\sigma = \sigma_s$ | $\sigma = 2\sigma_c$ | 24 | 14.8 | Doubling Initial Covariance |
| | 9 | $\sigma = \sigma_s$ | $\sigma = \sigma_c/2$ | 16 | 8.0 | Halving Initial Covariance |
| | 10 | $\sigma = \sigma_s/\sqrt{2}$ | $\sigma = \sigma_c/2$ | 16 | 8.0 | Halving Initial Covariance and Reducing Display Error |

* Additional Delay To Incorporate Go-Around Height Loss ~3 Sec

Numerical values for the "time-to-correct" for variations in ($\sigma_c$) and ($\sigma_s$) are given in Table 27. For example, in the baseline configuration (Case 1) it takes 14 sec. (see Table 27) to recover, on a $4\sigma$ basic (i.e., probability of catastrophe=$10^{-4}$), from the initial state covariance $\sigma_c$ (see Table 26) at fault detection, to the flare point window (see Table 28).

Typical plots of the recovery envelopes for altitude (a longitudinal axis state) and roll rate (a lateral axis state) are shown in Figures 21a and 21b, respectively. This figure illustrates typical post-fault recovery envelopes following the landing and go-round decisions. For a fault causing an upset in the lateral axis, the sequence of recovery actions is first to stabilize the aircraft in the lateral axis and then to execute a landing or a go-around.



(a) Longitudinal Axis - Vertical Deviation

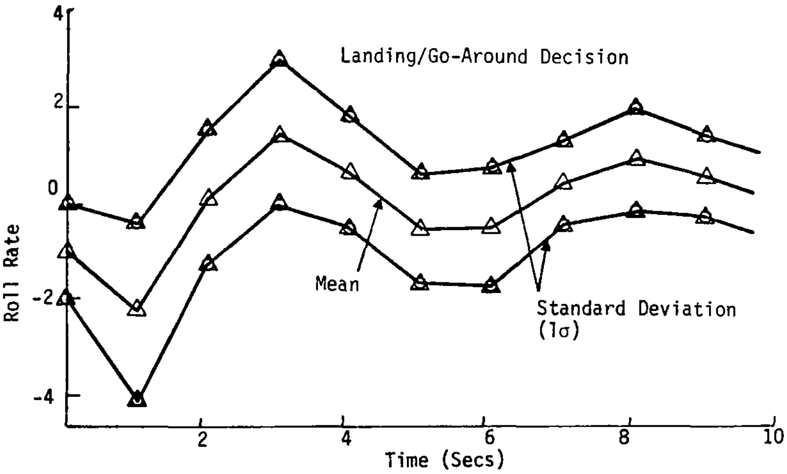


FIGURE 21.-FAULT RECOVERY COVARIANCE PROPAGATION EXAMPLES

TABLE 28.-ASSUMED AIRCRAFT RECOVERY LIMITS AND FLARE POINT WINDOW

| STATE | RECOVERY LIMITS | | FLARE POINT WINDOW | AXIS |
|---|---|---|---|---|
| | MAX | MIN | | |
| $\theta$, ° | 12 | 12 | ±0.5 | Longitudinal |
| u, - | 0.15 | -0.15 | ±0.02 | |
| $\alpha$, ° | +22 | -10 | ±0.5 | |
| q, °/s | 3 | -3 | ±0.05 | |
| L, m(ft) | 305(100) | -30.5(-100) | ±1.5(±5) | |
| $R_s$, m(ft) | 915(3000) | -610(-2000) | ±3.05(±10) | |
| $\delta_e$, ° | 10 | -5 | ±1 | |
| $\delta_{th}$ | 5000 | -500 | ±100 | |
| $\phi$, ° | 15 | -15 | ±1 | Lateral |
| $\psi$, ° | 15 | -15 | ±1.5 | |
| $\beta$, ° | 5 | -5 | ±1.5 | |
| p, °/s | 5 | -5 | ±0.5 | |
| r, °/s | 5 | -5 | ±0.5 | |
| L, m(ft) | 152(500) | -152(-500) | ±6.1(±20) | |

This sequence of actions is reflected in the recovery time listed in Table 27. Note that go-around recovery for a failure causing a lateral axis upset takes longer than that for a failure causing a longitudinal axis upset.

For the longitudinal and lateral axis, the principal conclusions are:

1. The go-around recovery covariance converges more rapidly than the landing recovery covariance.

2. The time to establish a positive rate of climb is of the order of one second and that covariance converges to 90 percent within three seconds. Note that these results must be used cautiously since they are based on linearized perturbation models.

3. The time required for the covariance to coverge increases with $\sigma_c$ and $\sigma_s$.

4. For a landing decision, the covariance takes as much as ten seconds to converge.

5. Because linear perturbation equations have been used, the go-around height loss does not show up on the plots.

6. The lateral axis recovery takes longer than the longitudinal axis recovery due to the additional time required to stabilize the aircraft laterally.

7. For the values of display error standard deviations ($\sigma_s$) considered, the recovery performance is insensitive to these errors.

In summary, for the particular set of numerical values used on detecting a failure, the safer decision is to execute a go-around. Recalling that the time to detect is no more than two seconds, the total time for longitudinal go-around recovery from fault initiation is about eight seconds. This compares favorably with current FAA requirements. It is noted that an emergency landing decision is warranted only if the time to touchdown is of the order of less than three seconds. To resolve conclusively the strategy details below the flare height, computer simulations (manned and unmanned) must be performed using detailed nonlinear models incorporating ground effects and aircraft configuration change effects at these heights.

# VI. TOTAL SYSTEM PERFORMANCE, ASSOCIATED STRATEGIES, AND DISPLAY REQUIREMENTS

Using the results generated by conducting the safety budget, fault detection and fault recovery analyses, this chapter evaluates total system performance and the resultant optimum pilot-crew ILM strategy. System performance is characterized by the total time (detection and recovery) curves for go-around and landing. This performance is characterized by the critical altitude (CA) and decision altitude (DA). These altitudes, in turn, define boundaries to the ILM strategies for go-around and manual landing initiation. Appropriate display concepts are proposed to implement the ILM strategy. The two distinct versions of these displays are the go-around prompter status display and the manual guidance display. Associated sensor and computational requirements are also considered in this context.

## Total System Performance

The total time curves for go-around and landing recovery are determined by summing together the time-to-detect and time-to-correct curves obtained from the fault detection and fault recovery analysis, respectively. Figure 22 shows a superposition of the time-to-detect curve for the variance change ($\chi^2$ test) algorithm (see Fig. 13) and the longitudinal axis fault recovery (time-to-correct) curve (see Table 27). These two curves are summed together for the same initial state error deviation ($\sigma$) ratio, along the time axis. The multiple of standard deviations ($\sigma$) to be used to assure that the probability of catastrophe during go around is $10^{-4}$, budgeted in Chapter III and Appendix B, was established as four standard deviations ($4\sigma$). The resulting total

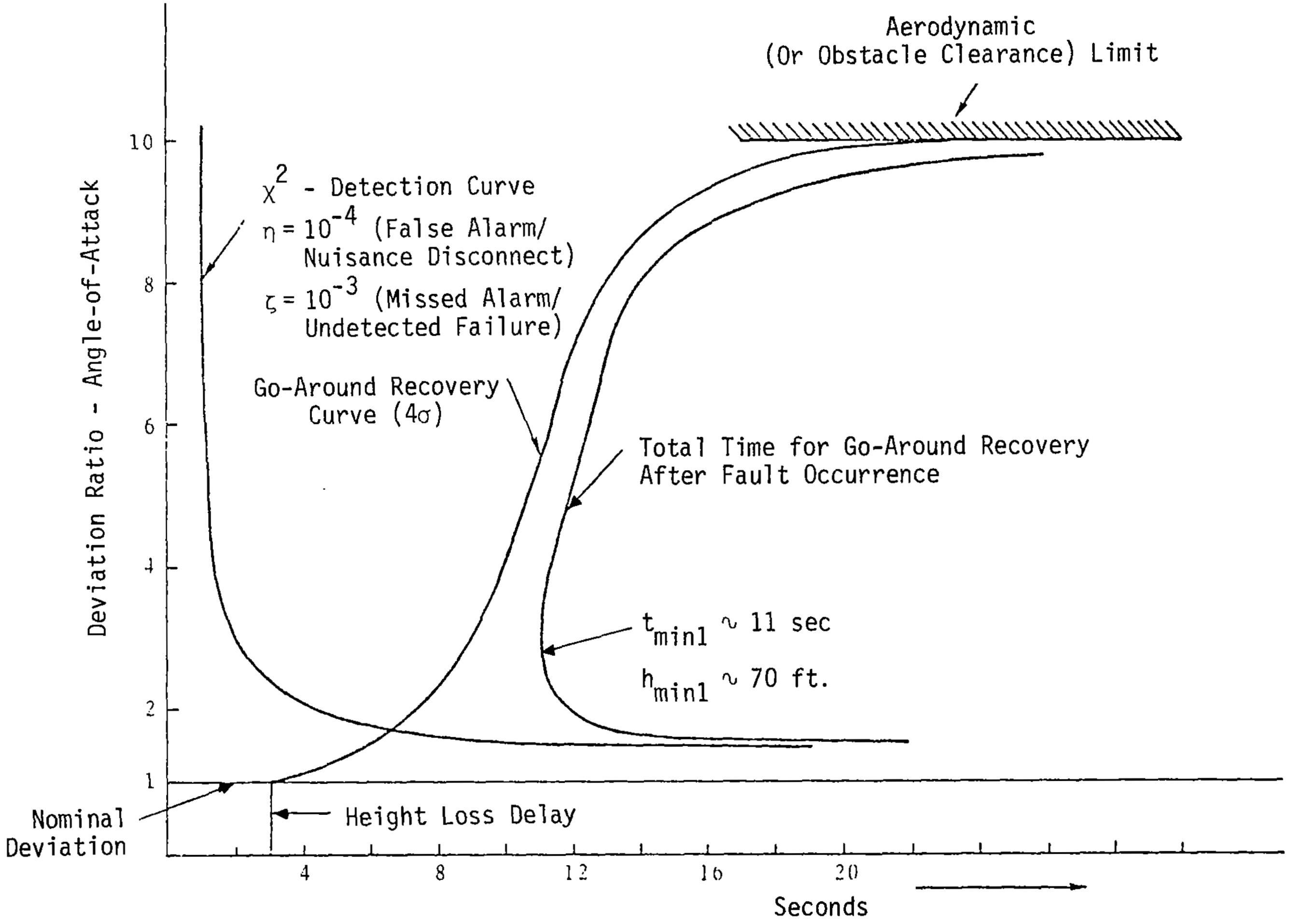


FIGURE 22.- DETERMINATION OF TOTAL TIME (DETECTION/RECOVERY) FOR GO-AROUND TASK (BASELINE) IN LONGITUDINAL AXIS

time curve shows that the tolerable deviation ratio due to faults, decreases until $t$ is less than or equal to $t_{\min 1}$. Below $t_{\min 1}$, no fault is tolerable without violating the required level of safety.

The altitude on the nominal profile at which the time to touch down is equal to $t_{\min 1}$, is defined as the critical altitude (CA). Below this altitude the pilot/crew must prepare for an emergency landing, in the event that a fault occurs. This is because the error state due to the fault would no longer be recoverable with a probability of catastrophe during go around of less than $10^{-4}$ (e.g., $4\sigma$ basis).

The "time-to-detect" and "time-to-correct" can be scaled up to correspond to five standard deviation values, for example, and then summed to yield a different total time curve. Using Table B-1 of Appendix B, this corresponds to a budgeted probability of go around catastrophe of $3.4 \times 10^{-6}$--a much safer go around. But the corresponding $t_{\min 1}$ from the new total time curve would be much larger. This illustrates the intuitively obvious concept that it is safer to execute a go around from a higher altitude (i.e., more time to touchdown).

The total time curve for landing recovery is obtained in a similar fashion, as shown in Fig. 23. For the particular set of numerical values used, the minimum time for landing recovery, $t_{\min 2}$, is equal to 22 seconds. The altitude at which the time to touchdown is $t_{\min 2}$ is defined as decision altitude (DA). Below decision altitude, no fault is sufficiently recoverable to execute a manual landing within the required levels of safety (i.e., $10^{-4}$).

The portion of the go around recovery curve, in Fig. 22, and the landing recovery curve,, in Fig. 23, corresponding to recovery

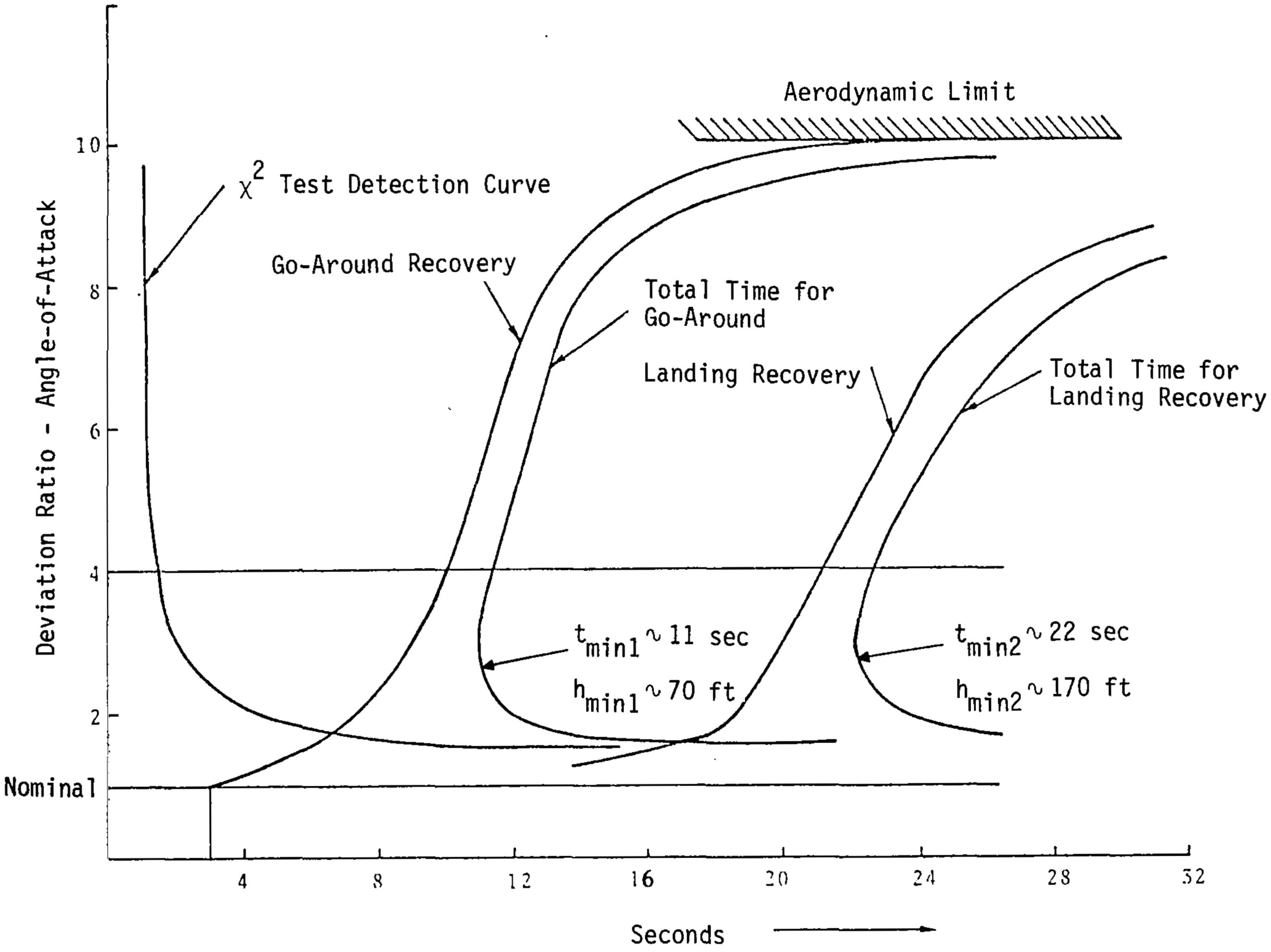


FIGURE 23.- COMPARISON OF TOTAL TIME FOR RECOVERY - GO-AROUND AND LANDING

from large initial deviations (i.e., large recovery time) is of dubious validity. One can reasonably expect that the linearized small perturbation models used for the aircraft and the pilot are no longer valid under large perturbations from the nominal. The characteristics of this portion of the curve must be obtained by performing an extensive Monte Carlo analysis on a cockpit simulator with a detailed nonlinear aircraft model.

For the lateral axis recovery case, the pilot stabilizes the aircraft prior to executing a go around or a landing. Referring to Table 27, this requires an additional amount of time equal to four seconds. Thus, the corresponding recovery time curves and the $t_{min}$'s would be increased by four seconds for recovery from a lateral axis fault, maintaining the same level of system safety.

The absissa of the total time curves (i.e., Figs. 22 and 23) obtained in this manner, are translated to an equivalent height using the nominal landing sequence time-height correspondence in Fig. 5 of Chapter II. The results of Figs. 22 and 23 enable one to superimpose the allowable deviation envelopes (ordinate in Figs. 22 and 23) on the nominal approach profile for each of the six longitudinal and lateral axis states. The allowable deviation envelope for one state, namely altitude, has been shown in Fig. 24. The critical altitude and decision altitude are 23 m (70 ft) and 56 m (170 ft), respectively, for the numerical values used in this example. These altitudes can be compared with the currently defined nominal "alert altitude" (i.e., altitude at which an autoland system must be fail operative to continue on automatic landing Category III weather) of about 26 m (80 ft), and the Category II "decision height" of 30.5 m (100 ft).

A figure similar to Fig. 24 can be obtained, for system performance, for lateral axis faults. Basically, the allowable deviations for the same altitude are reduced, and the critical decision

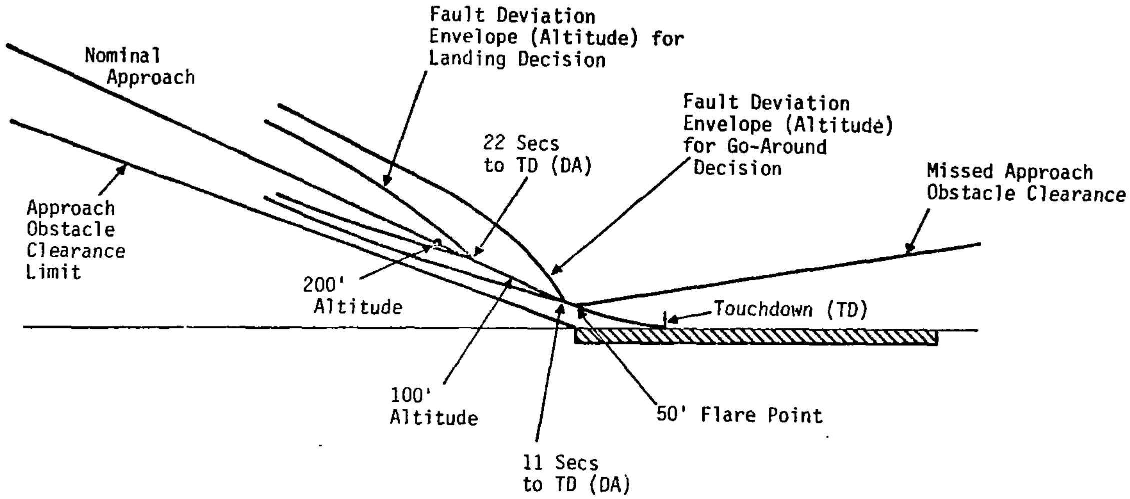

Fault Deviation Envelope (Altitude) for Landing Decision
Nominal Approach
Fault Deviation Envelope (Altitude) for Go-Around Decision
22 Secs to TD (DA)
Missed Approach Obstacle Clearance
Approach Obstacle Clearance Limit
200' Altitude
Touchdown (TD)
100' Altitude
50' Flare Point
11 Secs to TD (DA)

FIGURE 24.- COMPARISON OF ALLOWABLE LONGITUDINAL FAULT DEVIATION ENVELOPES

altitudes are increased to 30.5 m (100 ft) and 61 m (200 ft), respectively. These correspond to an additional recovery time requirement of four seconds above that for the longitudinal axis faults.

The ILM system information and display requirements, implicit in these recovery time and aircraft state deviation envelopes, are functions of the assumptions made in the previous chapters and the appendices. By virtue of its definition as the measurement equation, for example, Fig. 39 in Appendix B leads to the ILM sensor requirements. Information requirements arise from the need to detect and discriminate among possible failures; and display requirements arise from the need to provide the pilot with an adequate means of executing a "safe" recovery.

Sensor errors affect the state being measured in an RSS (root-sum-square) sense. To ensure that the contribution of sensor error statistics is negligible to the required false alarm $(\eta)$ and missed alarm $(\zeta)$ rates, the sensor measurement error standard deviation $(\sigma)$ is specified to be one-third of the nominal standard deviation of a particular state, due to environmental disturbances (note that $3\sigma$ for a univariate random variable is approximately 0.997). Thus, using Tables 24 and 26, a set of ILM information and display requirements can be derived, as in Table 29. Since extensive sensitivity studies were not conducted in this study, these requirements are of a preliminary nature.

The fault recovery portion of the results presented in this section have been derived from a linearized aircraft model about a particular nominal condition together with an optimal control pilot model with a hypothetical set of numerical parameters. Additional

TABLE 29: PRELIMINARY ILM INFORMATION AND DISPLAY REQUIREMENTS FOR STRATEGY A

| STATE | ACCURACY REQUIREMENTS ($1\sigma$) | | COMMENTS |
|---|---|---|---|
| | INFORMATION (DETECTION/ DISCRIMINATION) | DISPLAY (RECOVERY) | |
| Lateral | | | |
| L (Displacement) | 0.82 m (2.5ft) | 1.5 m (5 ft) | L ≡ y |
| $\psi$ (Heading) | 0.1° | 1° | |
| $\phi$ (Roll) | 0.1° | 1° | |
| $\beta$ (Sideslip) | 0.1° | 1° | |
| Longitudinal | | | |
| $\theta$ (Pitch) | 0.21° | 1° | |
| u (Airspeed) | 0.7 m/s (0.5 ft/sec) | 0.52 m/s (1.7 ft/sec) | $\dot{u}$ is proportional to $\dot{x}$ |
| $\alpha$(Angle-of-Attack) | 0.21° | 1° | |
| h (Altitude) | 0.3 m (1 ft) | 0.3 m (1 ft) | h ≡ z |
| $R_s$ (Slant Range) | 0.66 m (2.1 ft) | 1.5 m (5 ft) | |

work remains to be performed to study the sensitivity of recovery time curves to variations in aircraft and pilot model parameters. Nonetheless, the results presented are representative of the process of fault detection and subsequent fault recovery.

## ILM Usage Strategy

The basic computations of the total time constraints, critical altitude, and decision altitude can be translated into definitive strategies for operational usage of the Independent Landing Monitor. The four elements that must be considered in categorizing the type of usage are the navigation aid error characteristics of the runway, the landing accuracy performance requirements (i.e., touchdown dispersion manifold), the existing weather category, and the airborne autoland system configuration. Again, the type of usage ranges from a runway obstruction monitor/gross fault monitor to a system with "manual guidance to touchdown" capability.

Seven principal configuration categories are noted in Table 30. These categories address uses of an ILM in weather visibility ranging from Cat I to Cat IIIa. Cat 2½ is used to designate visibility conditions midway between Cat II and Cat IIIa.

These configurations have been arranged in the order of decreasing system performance capability and, therefore, cost. Configuration 1 represents the highest performance available from the navaid characteristics, landing accuracy required, and avionics reliability. Here, the principal usage of the ILM is to serve as a ground obstruction monitor and confidence builder. Thus, this function must be evaluated further by cockpit simulation or flight test.

In Configuration 2, the autoland equipment quality is downgraded by using less expensive but poorer quality components

TABLE 30.-CANDIDATE APPLICATIONS FOR AN ILM

| CONFIGU-URATION | NAVAID CHARACTERISTICS | LANDING ACCURACY PERFORMANCE | WORST WEATHER (ACTUAL) | AIRBORNE SYSTEM CONFIGURATION | ILM USAGE |
|---|---|---|---|---|---|
| 1 | Category III | Category III | Category IIIa (See To RollOut) | Fail Operative | Ground Obstruction Monitor; Confidence Builder |
| 2 | Category III | Category III | Category IIIa | Fail Operative (Downgrade Equipment Quality) | Detect Out of "Design Envelope" Conditions and Faults; Use Appropriate Strategy (Table 30) |
| 3 | Category III | Category III | Category IIIa | Fail Passive | " " |
| 4 | Category III | Category II | Category 2 1/2 Decision Height ∿ 50 Feet) | Fail Passive | " " |
| 5 | Category II | Category II | Category 2 1/2 | Fail Passive | Reduce Decision Height to. 50 Feet (Category 2 1/2); Go-Around If Fault Detected |
| 6 | Category III | Category II | Category 2 1/2 | Simple Monitoring | Reduce Decision Height; Go-Around If Fault Detected. |
| 7 | Category I/II | Category I/II | Category II | Simple Monitoring | Go-Around If Fault Detected; Applicable To General Aviation |

resulting in a higher equipment failure rate. Here, the ILM is used to "catch" the resulting higher rate of system failures. The intent would be that a lower overall system cost would result. This corresponds to designing a new aircraft configuration with less expensive primary avionics and an ILM effectively to buy back the loss of reliability.

Configuration 3 applies to fail-passive avionics configurations. Here, the objective of using the ILM is to upgrade safety to the point where the fail-passive system could be used for Cat IIIa operations.

Configurations 4, 5, and 6 illustrate the attempt to operate in poorer weather conditions than Category II but better than Category IIIa. This is economically attractive because such a weather condition is far more frequent than Category IIIa type weather. Thus, potentially, at a small equipment cost increase, a substantial operational gain can be made using an ILM. Condition 4 addresses lowering the decision height below the Cat II requirement by use of the ILM. Condition 5 addresses the same situation, except that the navaid system is certified only for Cat II rather than Cat III. Condition 6 is the same as Condition 5 except the autoland system is not fail-passive (i.e., the automatic disconnect feature is absent). Thus, it places the most stringent requirements on the ILM.

Configuration 7 applies to general aviation aircraft. Here, the intent is to lower the operational ceiling of the simple avionics system. Note that for Configurations 5, 6, and 7, the ILM is mainly used as a go around prompter. The configurations labeled 3, 4 and 5 are considered to be the most promising usage categories based on the projected numbers of aircraft and economic-operational benefit.

To specify clearly the operational strategy to be executed for each of these configurations, one needs to consider the type of fault that occurs and the height at fault detection. Table 31 presents the pilot/crew strategy for Configurations 2-7 in Table 30. Based on the fault type and detection height, this table

TABLE 31.- PILOT/CREW STRATEGY FOR EACH CONFIGURATION (POST FAULT DETECTION)

| CONFIG-URATION | HEIGHT AT FAULT DETECTION | FAULT/FAILURE | ILM ANNUNCIATOR | PILOT ACTION |
|---|---|---|---|---|
| 2,3 | h > DA | 1. Wind Outside Design Envelope | Abort | Initiate Automatic/Instrument Go-Around at h = DA |
| | | 2. Autoland or MLS Fault Leading to Landing Accuracy Performance Degradation (Down to Category II) | Caution | Continue Autoland Approach Until DA; Be Prepared for Go-Around<br>Exercise Instrument Landing With ILM Guidance or<br>Automatic/Instrument Go-Around |
| | | 3. Unacceptable Autoland/MLS Fault (Hard) | Abort | |
| | CA < h < DA<br>CA ∿ 6m | Case (1), (2), (3) | Abort | Automatic/Instrument Go-Around |
| | *0 < h < CA | Case (1), (2), (3) | Landing | Automatic/Instrument Land; Be Prepared To Initiate Emergency Landing Procedure |
| 4,5,6 | h > DA<br>DA ∿ 16m (Category 2-1/2) | 1. Wind Outside Design Envelope | Abort | Automatic/Instrument Go-Around |
| | | 2. Autoland or MLS Fault Leading to Landing Accuracy Performance Degradation (Down to Category I) | Caution | Continue Autoland/Instrument Approach Until DA; Establish Visual Contact to Land, Otherwise Go-Around |
| | | 3. Unacceptable Autoland/MLS Fault (Hard) | Abort | ILM/Instrument Guidance to DA; Establish Visual Contact and Land Manually; Otherwise Go-Around |
| | CA < h < DA<br>CA ∿ 6m | Case (1), (2), (3) | Abort | Automatic/Instrument Go-Around |
| | *0 < h < CA | Case (1), (2), (3) | Landing | Automatic/Instrument Land, Be Prepared To Initiate Emergency Landing Procedure |
| 7 | h > DA<br>DA ∿ 60m | Fault Detected | Abort | Instrument Go-Around |
| | h < DA | ---- | --- | Establish Visual Contact at DA and Land Manually |

*See Table 31 for strategy modification based on aircraft attitude specifies the required ILM annunciator display message and the corresponding pilot/crew strategy recommendation. The strategies are partitioned into three subgroups based on the system configuration, defined in Table 30. For each of these subgroups, the strategy is controlled by the altitude at which the fault occurs, as compared to the critical altitude (CA) and decision altitude (DA). Thus, three ranges of altitude h exist, namely: (1) $h > DA$, (2) $DA > h > CA$, and (3) $CA > h > 0$. Corresponding to each of these altitude zones, three main classes of faults can occur, namely: (1) wind outside design envelope, (2) autoland or MLS fault leading to landing accuracy performance degradation (down to Cat II), and (3) unacceptable autoland or MLS fault (hard failure). The corresponding pilot action is documented in the last column.

When the wind exceeds the design conditions above DA, the control remains automatic until DA is reached. If this wind condition has not subsided by the time DA is reached, an automatic instrument go-around is initiated. If the failure is soft, leading mainly to performance degradation, then the automatic approach is continued until DA with the proviso that if the nature of the fault becomes more severe, a go-around must be executed. If the nature of the fault remains the same, enough monitoring capability must be provided to the pilot to assure him that the automatic landing can be safely continued. If an unacceptable fault is detected for $h > DA$, then a manual takeover is required. Whether a go-around or a manual landing is executed depends on the guidance capabilities of the ILM system.

The principal difference between the strategy for Configurations 2 and 3, described above, from that for 4, 5, and 6 is that better visibility exists for the latter. Thus, post-fault manual landings are attempted only after establishing visual contact with the runway above DA for Configurations 4, 5, and 6. In all cases, for altitudes below DA but above the critical altitude (CA), the automatic landing is aborted and a manual go-around is initiated in case of detected fault.

For altitudes below the CA, further strategy modifications based on aircraft altitude are possible. Essentially, these amount to recommending that in the event of a pitch up situation due to a fault, it is better to execute a go-around rather than a landing, for the longitudinal axis. And if the roll attitude or roll rate due to a fault increases the lateral deviation , then the proper pilot action is go-around rather than land. This type of strategy refinement for low altitudes is documented in Table 32. The Boeing 737 attitude limits at touchdown, for a 3 m/s (10 f/s) sink rate are presented in Fig. 25. These attitude constraints can be extrapolated to slightly higher altitudes to define recommended pilot/crew actions based on aircraft attitude at fault detection. In this manner, the pilot/crew strategy at the higher altitude can be blended with those at lower altitudes.

## Proposed Display Configurations

The candidate ILM display configurations fall into two categories--automatic fault monitoring/warning and manual guidance. When the primary ILM mode is automatic warning and the secondary mode is pilot display, the monitor warns the pilot when the aircraft exceeds predetermined flight envelope limits. The secondary mode pilot display provides guidance under two conditions: (1) from failure warning point down to DA, and (2) from any warning point to a safe go-around flight path.

On the other hand, if the primary ILM mode is to serve as a pilot display for manual guidance, then it provides the pilot with a visual picture of where the aircraft is within the safe flight envelope. It also provides a "continue to DA" or go-around flight

TABLE 32.-STRATEGY REFINEMENT FOR ALTITUDES BELOW THE CRITICAL ALTITUDE

| AXIS | CONDITION | PILOT ACTION |
|---|---|---|
| Longitudinal | $\dot{\theta} > (\dot{\theta})_{max}$; $\theta > (\theta)_{max}$ | Go-Aronnd |
| | $\dot{\theta} < (\dot{\theta})_0$; $\theta < (\theta)_{max}$ | Land |
| Lateral | $L\phi > (L\ )_{max}$ | Go-Around |
| | $\phi\dot{\phi} < (\phi\dot{\phi})_{max}$ | Go-Around |
| | $L > L_{max}$ | Go-ARound |

Notation: $\theta$ - Pitch angle
$\dot{\theta}$ - Pitch rate
$\phi$ - Roll angle
$\dot{\phi}$ - Roll rate
L - Lateral displacement of centerline

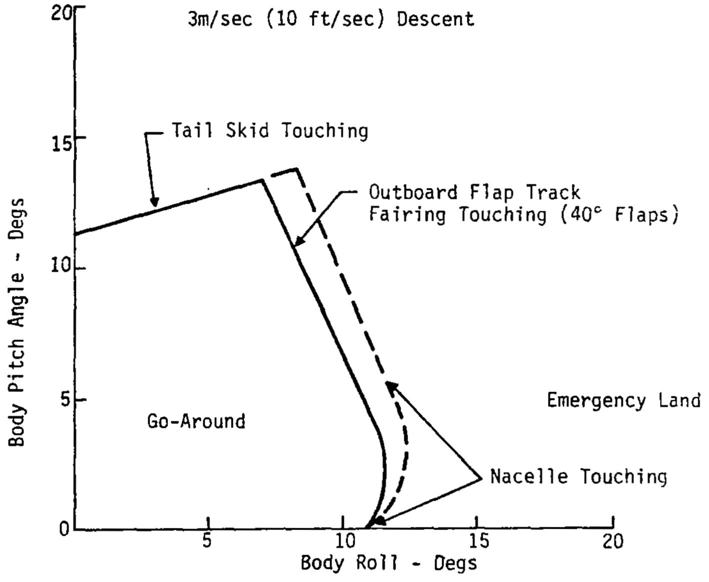


FIGURE 25. -TOUCHDOWN ATTITUDE LIMITS FOR THE BOEING 737-100

path guidance on command. The secondary automatic warning mode of the ILM, in this case, provides a backup warning if the pilot ignores the primary display mode.

The ILM system output in its simplest format would be a status panel-type display depicted in Fig. 26. Each of the status panel symbols correspond to those noted in Table 31, discussed in the previous section. The caution signal would typically be a flashing amber light cancelable by the pilot. The controlling logic would reinitiate the alarm if the hazard still existed after, say, three seconds. The other symbols in the panel would be flashing or steady red lights, cancelable only on executing the appropriate pilot/crew strategy described in Table 31. These basic visual signals could be augmented by the proper auditory (e.g., buzzer, synthetic voice) alarms.

An appropriate guidance mode display is illustrated in Figure 27. This display format is similar in configuration to current guidance/flight director displays except that an elliptic boundary representing the ILM safe manifold is added. This display would function as a continuous monitoring aid to the pilot during automatic landing. Go-around prompting and guidance are provided when a fault is detected. A fault is visually detected when the aircraft symbol falls outside the safe manifold ellipse.

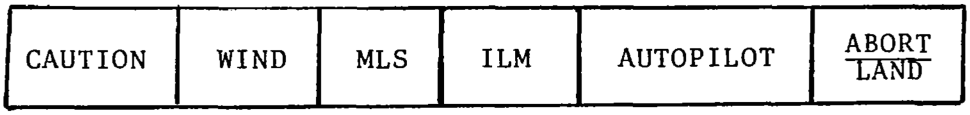


FIGURE 26.-STATUS-MONITOR PANEL IN ILM DISPLAY OPTION

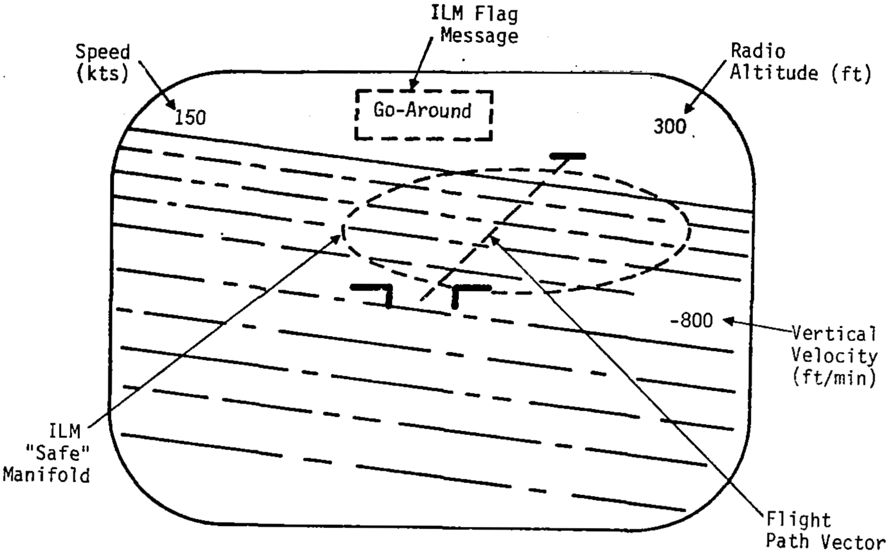


FIGURE 27a.-PILOT DISPLAY MODE - CRT DISPLAY (MONITOR/ GO-AROUND PROMPTER) -- AT INSTANT OF GO-AROUND INITIATION

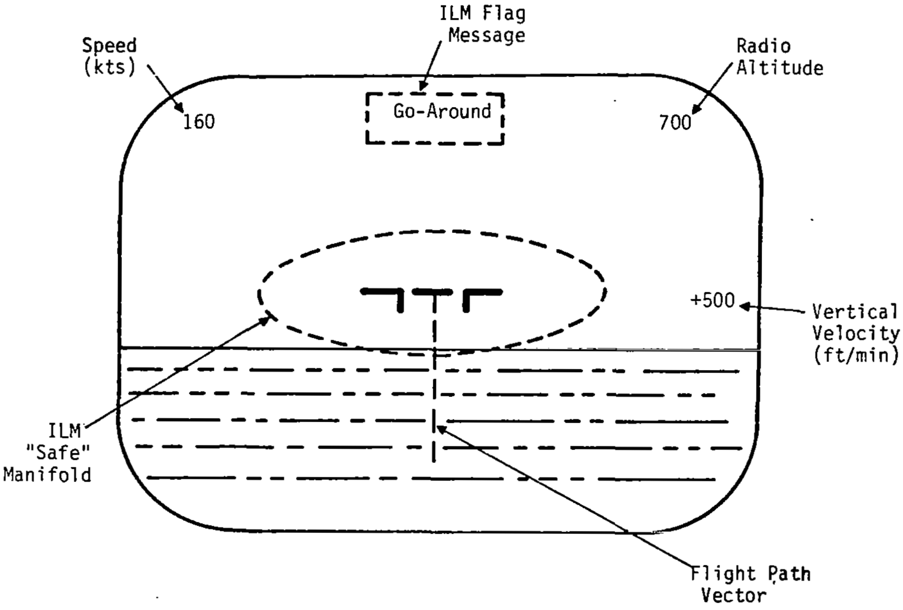


FIGURE 27b.- PILOT DISPLAY MODE - CRT DISPLAY (MONITOR/ GO-AROUND PROMPTER)--AT INSTANT OF GO-AROUND RECOVERY COMPLETION

Figure 27a shows the displayed situation at the time instant when the go-around is initiated due to the aircraft symbol falling outside the ILM "safe" manifold. A go-around flag is displayed at the top center of the display, and a flight path vector leading to safe recovery is indicated. The changes in symbology that occur at the time instant the go-around recovery is completed are shown in Figure 27b. Note that the ILM "safe" manifold is centered and a positive climb rate has been established.

For autoland equipped aircraft with landing guidance provided by the ILM, the display would incorporate a runway symbol to aid the pilot in assessing his relative position prior to decision height; a display of this type is presented in Figure 28. At the lower edge of the display, the ILM derived smoothed runway reference heading is displayed. On the left edge, the smoothed flight

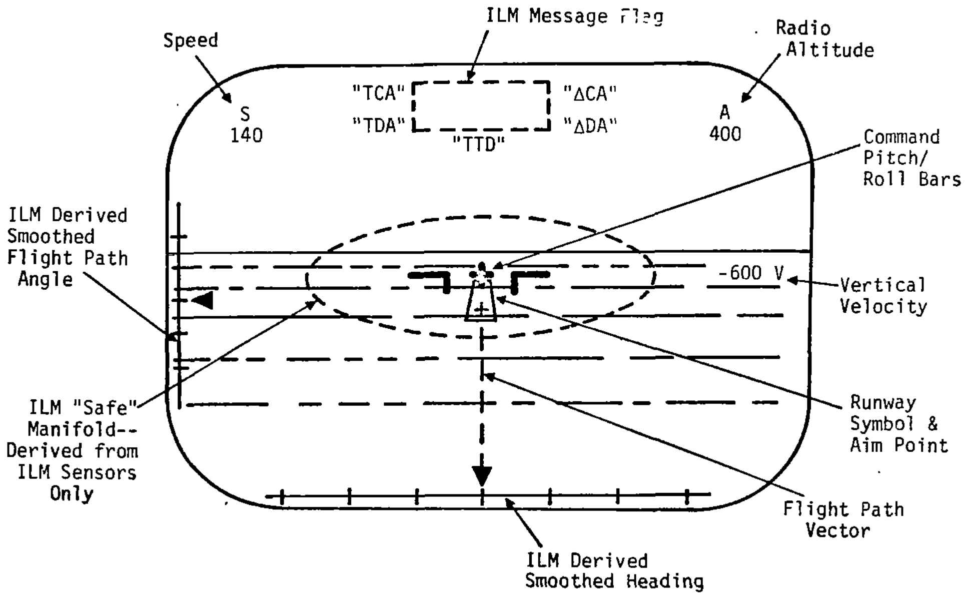

ILM Message Flag
Speed
Radio Altitude
S
140
"TCA"
"TDA"
"TTD"
"ΔCA"
"ΔDA"
A
400
Command Pitch/ Roll Bars
ILM Derived Smoothed Flight Path Angle
-600 V
Vertical Velocity
ILM "Safe" Manifold-- Derived from ILM Sensors Only
Runway Symbol & Aim Point
Flight Path Vector
ILM Derived Smoothed Heading

FIGURE 28.- CANDIDATE LANDING DISPLAY FORMAT FOR ILM SYSTEM (AUTOLAND NORMAL)

path angle is displayed. The heading and flight path angle information are supplemented by a flight path vector and aim point display superimposed on the runway symbol, during the last 300 m (1000 ft) of altitude. At 300 m altitude, the ILM messages at the upper-middle portion of the display are activated.

The central portion of the display in Figure 28 contains a specific message such as "go-around" or "land." The objective of this message field is to integrate the status type information regarding faults detected and the corresponding pilot decision into a single CRT type display. On the left of the message field, the time to critical altitude (TCA) and time to decision altitude (TDA) are displayed. On the right side of the field, the difference between current altitude and critical altitude (ΔCA), and current altitude and decision altitude (ΔDA) are displayed. These four numbers provide the pilot with continuous information on the emergency alternatives available to him (if a fault were to occur) and the criticality of a fault. For example, an autoland failure above decision altitude would allow him to take over and land safely, whereas such a failure below decision altitude would require the pilot to execute a go-around. An additional quantity displayed to the pilot is the time to touchdown (TTD); this becomes the key parameter of interest below critical altitude.

Additional parameters to be displayed would include: (1) command pitch, roll, and speed bars, and (2) estimated wind and turbulence level. The final design format for displays to execute manual landings to touchdown under low visibility conditions must await a substantial cockpit simulation effort backed by computer analysis.

For the aircraft not equipped with automatic landing capability, the ILM serves as an autopilot monitor. The display symbology is similar to that for autoland aircraft. The differences are a direct result of differing usage strategies. The main objective of an ILM in this case is to: (1) provide visual guidance down to DA, and (2) command a go-around in case of equipment failure or severe winds. The display format in Fig. 29a depicts the situation when the aircraft is at the caution limits and manual takeover procedures must be initiated. Figure 29b presents the situation where the "caution" flag has been changed to "proceed to DA" requiring a manual takeover and ILM guidance to decision altitude; visual contact with the runway is to be established at that point before proceeding any further. The third situation shown in Fig. 29c indicates where the aircraft has deviated off the nominal by a significant amount and, consequently, the ILM message recommends a "go-around" rather than a "proceed to DA." Note that the "TDA" and "ΔDA" numeric message are no longer valid and are electronically removed from the electronic CRT display.

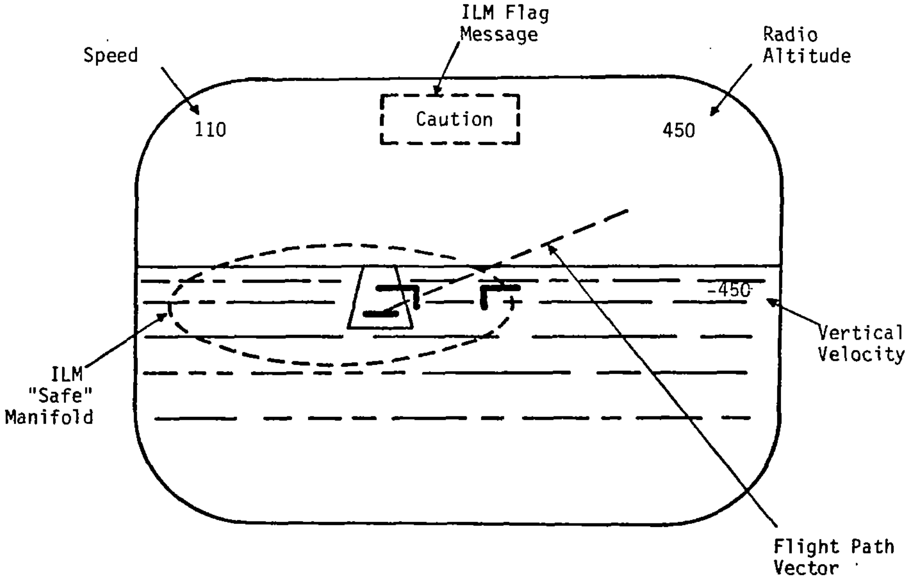


FIGURE 29a.- GUIDANCE MODES FOR NONAUTOLAND AIRCRAFT--AT CAUTION LIMITS

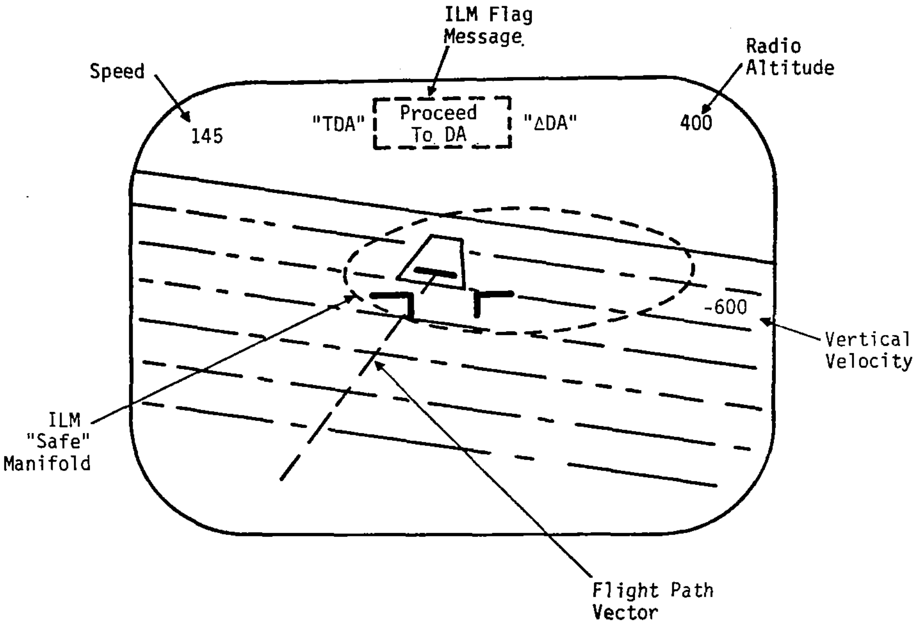


FIGURE 29b.- GUIDANCE MODES FOR NONAUTOLAND AIRCRAFT--PROCEED TO D.A. MANUALLY

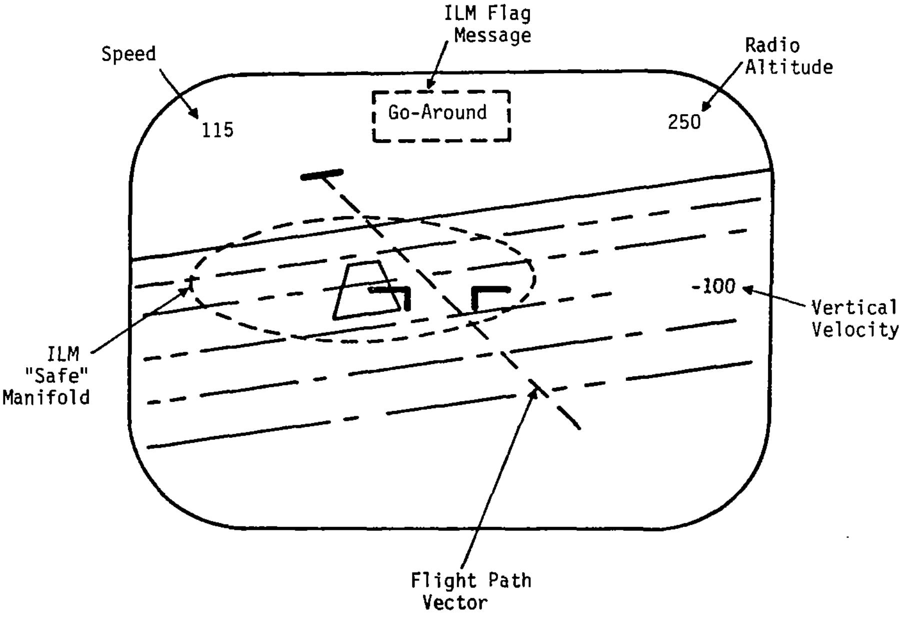


FIGURE 29c.- GUIDANCE MODES FOR NONAUTOLAND AIRCRAFT--EXCEEDING LANDING LIMITS, MANUAL GO-AROUND MODE

## System Hardware Implementation

Based on the material presented in the preceding sections of this report, an ILM hardware implementation is proposed. It consists of sensors for attitude and position with respect to the runway, a computer for implementing fault detection-discrimination algorithms and generating display information, and the displays for presenting the recommended pilot-crew action and fault category.

A schematic block diagram of the ILM computer with the associated input and output is shown in Figure 30. This figure indicates the ILM sensor inputs; these include independent position and attitude sensors.

Potential independent position sensors include: (1) precision approach radar, (2) trilateration transponders, and (3) redundant MLS. Attitude sensors recommended include redundant gyros to obtain roll ($\phi$), pitch ($\theta$) and heading ($\psi$) angles. Additional vane type or multiorifice head sensors are recommended for measuring angle-of-attack ($\alpha$) and angle of sideslip ($\beta$). The state manifold

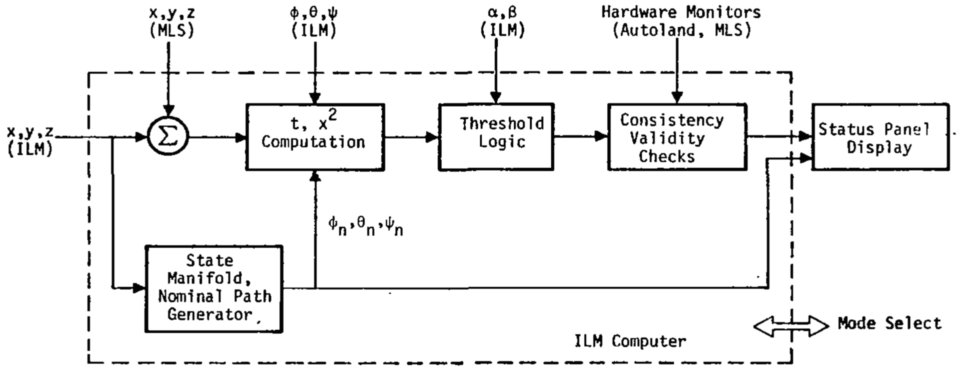


FIGURE 30.-SCHEMATIC BLOCK DIAGRAM OF AN ILM COMPUTER CONFIGURATION

generator computes the nominal roll ($\phi_n$), pitch ($\theta_n$) and heading ($\psi_n$) angle values for comparison with the measured attitudes.

The figure also shows the interconnections with the primary autoland and MLS systems and their sensors. In a practical implementation, a special effort must be made to minimize this interface. On the right side of the figure, the output to the display and mode selector panel is shown. The mode selection feature is included to allow the crew the ability to select the phase of flight and the guidance or monitoring mode described in the previous section on displays.

A considerable amount of further work remains to be performed (via analysis and cockpit simulation) before the ILM hardware configuration can be detailed. Specific items include finalization of intended uses for the ILM, establishment of fault detection algorithm details, establishment of ILM sensor configuration and accuracy requirements, refinement of display formats, development of ILM computer algorithms and logic requirements, and selection of computer, display, and interface requirements.

# VII. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

This effort has developed a systematic procedure which can be used to obtain specific information and display requirements for an Independent Landing Monitor. Numerical values and linearized system models were used throughout the study to test this procedure and to yield approximations to the ILM requirements for the Boeing 737 TCV aircraft.

The study had multiple objectives; briefly, these were:

1. Define the possible uses for the ILM and determine how these uses could be justified.

2. Establish the information processing requirements for the ILM that will support these uses. This included detection of faults in the MLS and autoland systems and out-of-tolerance wind conditions.

3. Determine typical time elapsed between fault occurence, fault detection, and fault recovery. The associated perturbation to the nominal flight path due to the fault was to be computed. Crew action included the manual takeover for both go-around and landing.

4. Based on the timing requirements, devise ILM strategies to govern what crew action is appropriate as a function of altitude and aircraft attitude.

5. Devise display formats that provide the crew with necessary information to monitor the automatic landing, determine that a fault has occurred, and guide the subsequent manual control of the aircraft.

6. Describe further analysis and testing required to realize the implementation of the ILM.

Because there are multiple, complex facets of the analysis of the ILM, this limited study concentrated on the final landing portion of the flight sequence. ILM uses for approach, rollout, and takeoff monitoring and guidance were briefly discussed but not analyzed.

## Summary and Conclusions

The use of the ILM studied in this investigation was to serve as a backup fault monitor and to provide guidance for manual fault recovery. The types of information that are derived by the ILM for such applications include: (a) the status of aircraft states, (b) the presence of a fault, (c) the type of fault, (d) what recovery strategy should be followed, and (e) pilot/crew guidance information to realize the recovery strategy. The manner in which this information is presented to the pilot and crew constitutes the display requirements.

The development of the information and display requirements involved a five-step iterative process. The steps were:

1. Determination of the ILM system performance requirements to meet fixed safety constraints. ILM performance is measured in terms of ILM hardware reliability, false alarm rate, and undetected failure rate.
2. Determination of time-to-detect specific fault situations with the ILM system performance (determined in the first step) fixed. This necessitated the postulation of fault detection algorithms and their subsequent simulation.
3. Determination of the time-to-correct the state error following the detection of the fault. The state error magnitude at the time of fault detection was dependent upon the required time for detection and the error growth rate due to the fault.
4. Specification of crew procedures following fault detection. These procedures were dependent upon the time availability for recovery in terms of remaining altitude and the prevailing conditions of the avionics, navigation aids, and environment (wind, visibility).
5. Recommendation of display formats that would provide necessary information to the crew to implement the previously specified procedures.

These steps are now summarized in more detail.

The ILM potentially has three general benefits -- improving the level of safety of an existing flight system, providing the means of lowering the landing minimums while maintaining a given level of safety, and providing the means of lowering the redundancy requirements (and thereby initial investment and maintenance costs) of the autoland system while still maintaining a given overall safety level. Thus, safety is an important criterion in the ILM design, and it is used in the study to specify hardware and software requirements for the ILM.

The system safety analysis required the determination of contribution of each flight subsystem to the total system probability of catastrophic failure. The introduction of an ILM to compliment a given autoland system must provide an improved level of safety based on the present standards for automatic landing systems. The analysis showed that for typical failure rates of existing equipment, the ILM could improve performance if a voting strategy was used where the ILM monitor had to agree with existing autoland or MLS monitors before corrective action was taken.

The safety budget analysis led to the specification of typical performance requirements for the ILM system. A landing phase (total exposure period) of 250 seconds was assumed, and the autoland/MLS equipment failure rate ($P_{EF}$) was assumed to be $10^{-4}$. (MTBF of 700 hours). The autoland/MLS hardware monitor false alarm rates (nuisance disconnects) and missed alarm rates (undetected failures) were assumed to be $10^{-3}$. The resultant ILM system performance requirements are as given in Table 33. These numbers produce an overall catastrophic accident rate of $10^{-6}$. Typical values are given for the ILM hardware failure rate ($P_{ILM}$), false alarm rate ($P_{FAI}$), missed alarm rate ($P_{MAI}$), go-around accident rate ($P_{GAI}$), and manual landing accident rate ($P_{MLI}$). These values are highly dependent on the assumed performance of the system without the ILM.

TABLE 33.-SAFETY BUDGET ANALYSIS REQUIREMENTS ON ILM SYSTEM PERFORMANCE

| PROBABILITY QUANTITY | NUMERICAL VALUE |
|---|---|
| Autoland/MLS Equipment Failure Rate (MTBF 700 Hours); ($P_{EF}$) | $10^{-4}$ |
| ILM Hardware Failure Rate ($P_{ILM}$) | $10^{-4}$ |
| ILM False Alarm Rate ($P_{FAI}$) | $10^{-4}$ |
| ILM Missed Alarm Rate ($P_{MAI}$) | $10^{-3}$ |
| Go-Around Accident Rate with ILM ($P_{GAI}$) | $10^{-4}$ |
| Manual Landing Accident Rate With ILM ($P_{MLI}$) | $10^{-4}$ |

The ILM false alarm and missed alarm requirements serve as constraints in designing the fault detection software. Specifically, these two numbers determine what threshold settings should be placed on the input measurements monitored and how many sequential samples of measurement data are necessary to determine that a fault has occurred. Conversely, for a fault to be detected in, say, two seconds, the false alarm and missed alarm constraints determine how much larger the state error due to the fault must be than the normal noise threshold of the measurement quantity. This governs the requirement placed on the ILM input measurement accuracy.

Two fault detection schemes, the t test and the $\chi^2$ test, were formulated for detecting abnormal changes in a measurement input's mean and variance, respectively. These schemes were tested by simulation to confirm that the false and missed alarm requirements were being met and that the time-to-detect matched analytical predictions. Additional schemes were suggested but not tested for discriminating the type of failure that did occur (e.g., autoland, MLS, wind gust).

The type of fault, the resultant rate of state error buildup, and the time-to-detect this fault determine how large the state error is at the time of fault recovery. Thus, the time-to-recover from a fault is dependent upon the time-to-detect. The time-to-recover is also dependent upon what action the pilot takes for the recovery. For the go-around, the action is first to stabilize the aircraft and then to execute the climb-out procedure. For manual landing, the aircraft is first stabilized, the desired glide slope is next captured, and finally this glide slope must be tracked.

To determine time-to-recover, a linear model was developed of the aircraft/display/pilot system. The different phases of the recovery required developing correspondingly different models of the pilot's action for each of these phases. The effect of ILM display errors were also included in the model. The pilot models were developed using the optimal control model procedure and limited available pilot performance data.

The linear system model was used to develop a covariance propagation procedure for assessing time-to-recover. Time-to-recover was defined as the length of time required to bring the aircraft error covariance inside of that which would normally exist due to normal gust conditions and navigation errors. This response time is highly dependent on the pilot performance model and what constitues "safe" recovery. Thus, the quantitative results of this study are only examples and must be substantiated by further cockpit simulator tests.

The accuracy requirements on specific states which are first used as inputs to the ILM and then are displayed to the crew for ILM Strategy A were obtained and are tabulated in Table 34. Essentially the ILM state input accuracy requirements are those dictated by the fault detection and discrimination system. The display parameter requirements are dictated by the recovery guidance needs during go-

TABLE 34.- PRELIMINARY ILM STATE INPUT AND DISPLAY REQUIREMENTS FOR STRATEGY A

| STATE | ACCURACY REQUIREMENTS ($1\sigma$) | | COMMENTS |
|---|---|---|---|
| | STATE INPUT (DETECTION/ DISCRIMINATION) | DISPLAY (RECOVERY) | |
| Lateral | | | |
| L (Displacement) | 0.82 m (2.5ft) | 1.5 m (5 ft) | $L \equiv y$ |
| $\psi$ (Heading) | 0.1° | 1° | |
| $\phi$ (Roll) | 0.1° | 1° | |
| $\alpha$ (Angle of Sideslip) | 0.1° | 1° | |
| Longitudinal | | | |
| $\theta$ (Pitch) | 0.21° | 1° | |
| u (Airspeed) | 0.7 m/s<br>(0.5 ft/sec) | 0.52 m/s<br>(1.7 ft/sec) | u is proportional to $\dot{x}$ |
| $\alpha$ (Angle-of-Attack) | 0.21° | 1° | |
| h (Altitude) | 0.3 m (1 ft) | 0.3 m (1 ft) | $h \equiv z$ |
| $R_s$ (Slant Range) | 0.66 m<br>(2.1 ft) | 1.5 m<br>(5 ft) | |

around and manual landing. Because extensive sensitivity studies were not conducted to study the effect of key parameters, these accuracy requirements must be treated as preliminary.

The time-to-detect and time-to-correct results were summed to yield total time for detection and correction as a function of state error magnitude. This was done for both lateral and longitudinal modes and both go-around and landing. These timing requirements were then converted to envelopes about the nominal approach trajectory. Constraints such as obstacle clearance, stall angle, and roll angle limits were imposed on these results. Thus, these envelopes defined altitudes above which it was safe to attempt a manual landing and safe to attempt a manual go-around. Two altitudes -- decision altitude (DA) and critical altitude (CA) -- were then defined which aided in the subsequent crew procedure definition.

The pilot decision strategy was then developed to correspond to the flight path envelope constraints, determined by the fault detection and recovery analysis. Three different variations of this strategy for Category II and IIIA weather, are summarized in Table 35.

Two different display concepts were developed to provide necessary monitoring and guidance information to the crew to allow mechanization of the ILM concepts developed in this study. Crew procedures are defined for using both displays. One display system consists of a set of panel warning lights shown in Figure 31, which would indicate which subsystem has failed, and what action is recommended to the crew. For this system, guidance would be provided by other cockpit instruments. The other display system proposed consists of a CRT-type display presented in Figure 32, showing the aircraft's attitude and position with respect to the nominal trajectory. A closing ellipse on the display indicates the boundaries of the safety envelope developed by the fault detection and recovery analysis. Additional features incorporated into the display include numeric data on the difference between the current altitude and the decision and critical altitudes (i.e., ΔDA, ΔCA), respectively; the corresponding time to reach these altitude is also displayed (i.e., TDA, TCA). These features enable the pilot/crew to be appraised of the recovery decision options that are open (i.e., go-around, manual landing with ILM, manual landing under visual guidance, emergency landing) at any given time. This display would have enough additional information to allow complete manual guidance for go-around or continuation of the landing sequence.

In summary, the main emphasis of this study was to establish a fundamental methodology for the analysis of landing systems (automatic or manual). The principal benefit of this analytical procedure is in generating design guidelines for implementing airborne

TABLE 35.-EXAMPLE POST FAULT DETECTION PILOT DECISION STRATEGY

| WEATHER CATEGORY | FAULT DETECTION ALTITUDE | PILOT/CREW ACTION | COMMENTS |
|---|---|---|---|
| II (Visible Below DA) | $h > DA$ | Proceed to DA Under Manual/Instruments | ILM Serves As Go-Around Prompter |
| | $CA < h < DA$ | Go-Around | |
| | $h < CA$ | Emergency Landing | |
| IIIA | $h > CA$ | Go-Around | ILM Serves As Go-Around Prompter |
| | $h < CA$ | Land; Prepare For Emergency | |
| IIIA | $h > DA$ | Manual Takeover And Land With ILM Guidance | ILM Provides Possible Guidance Capability To Touchdown In Category IIIA |
| | $CA < h < DA$ | Go-Around | |
| | $h > CA$ | Emergency Landing | |

Critical Altitude (CA) - Altitude below which no fault can be recovered from within required levels of safety, for a go-around or a landing decision.

Decision Altitude (DA) - Altitude below which no fault can be recovered from within required levels of safety, for a landing decision.

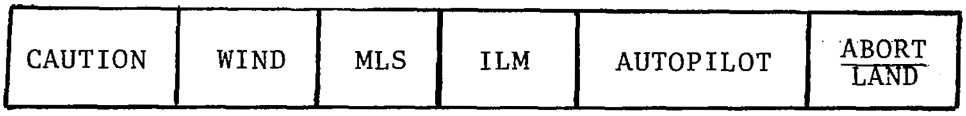


FIGURE 31.-STATUS-MONITOR PANEL IN ILM DISPLAY OPTION

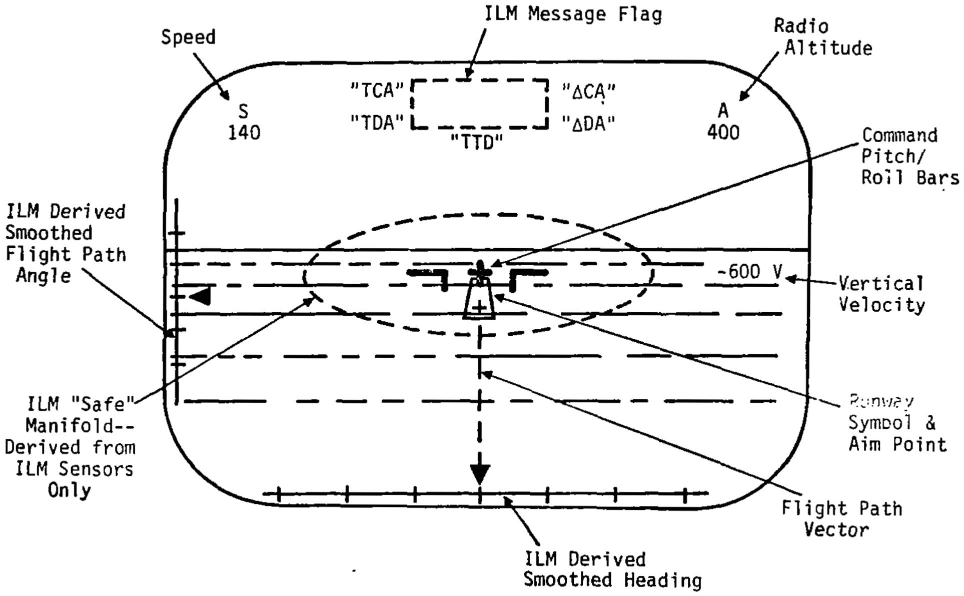

ILM Message Flag
Speed
Radio Altitude
"TCA"
"ΔCA"
S
140
"TDA"
"ΔDA"
A
400
"TTD"
Command Pitch/ Roll Bars
ILM Derived Smoothed Flight Path Angle
-600 V
Vertical Velocity
ILM "Safe" Manifold-- Derived from ILM Sensors Only
Runway Symbol & Aim Point
Flight Path Vector
ILM Derived Smoothed Heading

FIGURE 32.-CANDIDATE LANDING DISPLAY FORMAT FOR ILM SYSTEM (AUTOLAND NORMAL)

systems that would be too dangerous and costly to be obtained from flight test directly. Moreover, it provides a basis for formulating simulator experiments in a cost-conscious manner. Specific analytical results, of operational value, that can be obtained by applying this methodology include numerical values for landing minima and flight path deviation envelopes for a given aircraft/avionics configuration, ground-based navigation aid, and weather/visibility conditions. Furthermore, optimum (in a probabilistic sense) emergency recovery procedures can be derived as a useful byproduct of this methodology.

The analytical approach developed was used to evaluate information and display requirements for an ILM. It is emphasized again that many simplifying assumptions were used in this study for quantifying both the aircraft and pilot behavior and for determining the ILM performance requirements. These assumptions were necessary so that the methodology could be demonstrated and because detailed models (with numerical values) of the Boeing 737 TCV system were unavailable. Consequently, more anlaytical results should be obtained to get sensitivity measures of key parameters to the information and display requirements.

## Recommendations

Much additional work is required to reach a point where an ILM system based on the concepts of this study can be developed for flight testing. Seven specific study areas which require further work to enable designing and testing an ILM that meets broad usage requirements are:

1. Pilot Reaction Time--The timing requirements and manual landing/go-around decision logic are based on models for the pilot as a controller and decision maker. In this

effort, pilot models were based on limited previous data. An analytical/experimental effort is required to develop and validate more accurate models of the pilot response in stabilizing the aircraft and recovering from a fault condition. Model parameters must be determined that are consistent with the dynamics of the 737 aircraft in approach, landing, ground roll, and go-around. This modeling study would require extensive use of a cockpit simulator.

2. Ground Phase Analysis -- The current effort was mainly concerned with the landing phase (500 feet to touchdown) of flight. The ILM can also provide both lateral and longitudinal guidance during rollout and takeoff. Further analytical work is required to develop more detailed performance requirements of the system during this ground phase to supplement those developed in this study for the landing phase.

3. Approach and Go-Around Phase Analysis -- The ILM can be used during the approach phase as a ground proximity warning system and to detect general variations from the flight path. It can also be used as a backup guidance system during go-around. Similar to the ground phase, more analytical work is required to specify performance requirements for these phases.

4. Fault Detection -- The current effort defined methods which can be used to detect faults of the MLS, autoland, or ILM systems. The effort was based upon assumed measurement system models. Additional effort is required to obtain more exact models of sensor and signal inputs, their errors and noise characteristics, and the resultant effect on the performance of the fault detection logic. These more detailed results are required for specifying sensor accuracy requirements so that fault detection timing requirements can be met. Also, more specific software requirements must be determined.

5. Display Format Experiments -- Both headup and headown displays are being considered for the ILM. Further details as to the type and quantity of information displayed must be answered. A simulator experiment must be conducted to determine what the preferred format is with respect to pilot workload, pilot acceptability, and pilot performance in making decisions and controlling the aircraft. The required accuracy of the displayed elements must also be determined on an experimental basis. The fundamental question of whether the ILM can be used as a display for manual landing in Category III weather must be answered.

6. Timing Requirements -- The current effort required the assumption of preliminary pilot models and a linearized model of the 737. It also was assumed that the detection logic functions in a given time period. The completion of the effort described in Tasks (1)-(5) above would provide more exact information on the overall requirements of the ILM. In addition, more exact nonlinear models of the 737 aircraft are under development. More elaborate numerical methods exist which can be used to determine the statistical distribution of aircraft path perturbations due to faults. These elements should be combined in a detailed simulation to obtain more precise timing requirements for the ILM to detect faults in order to provide a specified level of safety.

7. Integration of Sensor, Computer, and Display Requirements -- The sensor, system software, and display requirements will dictate what type of computer is required to implement the ILM. Before proceeding to build a prototype of the system, a design study must be conducted to integrate the components and to provide the final design specification.

These seven tasks represent an integrated procedure which must be followed for development of an ILM that meets the wide range of potential users' requirements. These tasks are based on the systematic procedure developed in this study and other parallel work that has been accomplished. These steps serve to obtain more exact answers and to obtain quantitative and qualitative data that can only be produced by man-in-the-loop simulator studies.

The ILM has a great potential for reducing aircraft operating costs by allowing increased operation in low visibility conditions. However, to realize this potential requires a vigorous research and development program with a full committment on the part of the government to obtaining required technical and operational information. Specifically, a systematic simulator validation program must be conducted to verify the various assumptions made during the course of this study. It is recommended that such action be taken based on the steps outlined above.

# APPENDIX A
# SAFETY BUDGET ANALYSIS

## Introduction

In Chapter III the system safety assessment was presented using an event outcome tree. This tree is illustrated in Figure 33. The purpose of this appendix is to define in more methematical detail the meaning of the various types of probabilities which are included and relate these to the exposition in Chapter III. These definitions are related to safety requirements of the ILM monitor system.

The outcome tree relates only to the final portion of the landing approach. It is assumed that a critical altitude h* exists in the monitor logic. Above h*, the chances of a succesful go-around maneuver following a fault are greater than the chances of a successful landing. Thus, if the fault is detected above h*, a go-around maneuver is always commanded (and assumed to be obeyed); this is illustrated in Figure 34, as pilot decision Strategy A. Another strategy alternative, designated as decision Strategy B, is illustrated in Figure 35. This is a viable strategy provided the weather conditions permit adequate visual contact to be established with the runway prior to reaching altitude $h_2^*$.

The next section defines the various probability terms. Then equations to compute the terms defined are presented. The incorporation of an independent landing monitor (ILM), in addition to the existing primary autoland monitors, is discussed. Additional definitions and equations are also presented.

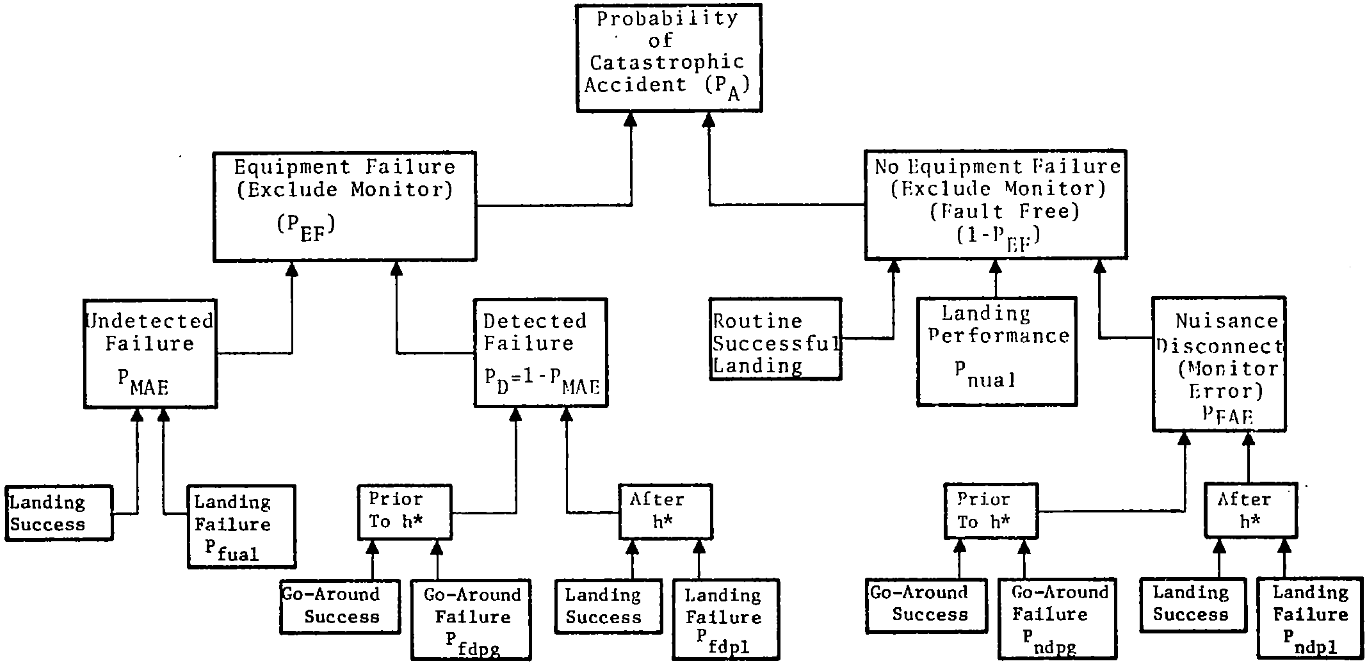

Probability of Catastrophic Accident ($P_A$)
Equipment Failure (Exclude Monitor) ($P_{EF}$)
No Equipment Failure (Exclude Monitor) (Fault Free) ($1-P_{EF}$)
Undetected Failure $P_{MAE}$
Detected Failure $P_D=1-P_{MAE}$
Routine Successful Landing
Landing Performance $P_{nual}$
Nuisance Disconnect (Monitor Error) $P_{FAE}$
Landing Success
Landing Failure $P_{fual}$
Prior To h*
After h*
Go-Around Success
Go-Around Failure $P_{fdpg}$
Landing Success
Landing Failure $P_{fdpl}$
Prior To h*
After h*
Go-Around Success
Go-Around Failure $P_{ndpg}$
Landing Success
Landing Failure $P_{ndpl}$

FIGURE 33.- EVENT OUTCOME TREE FOR MONITOR OPERATION DURING AUTOMATIC LANDING USING STRATEGY A.

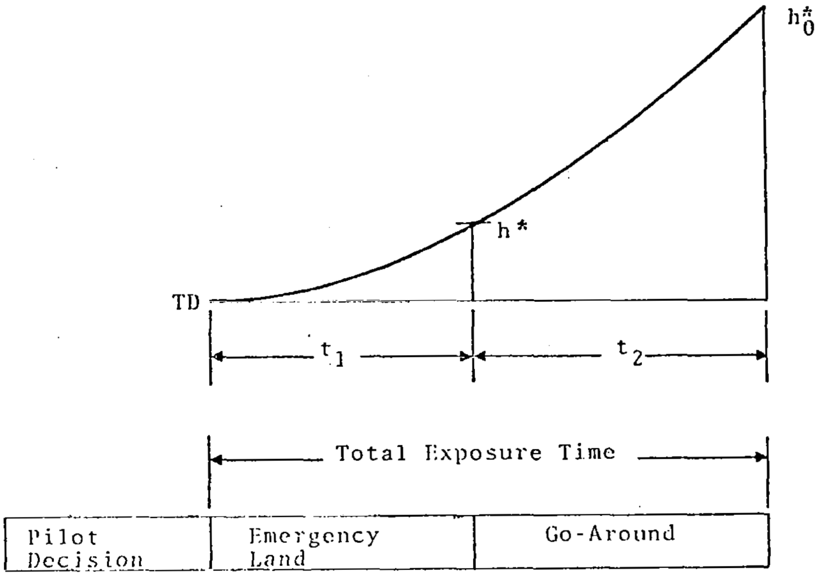


FIGURE 34.- POST FAULT DETECTION PILOT DECISION STRATEGY (A)

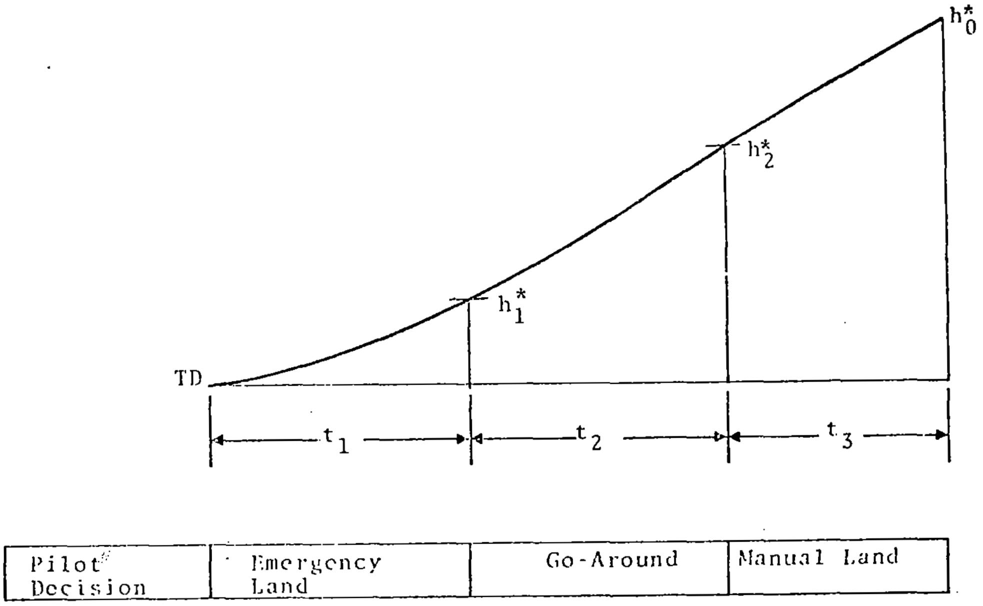


FIGURE 35.- POST FAULT DETECTION PILOT DECISION STRATEGY (B)

## Probability Definitions

To understand the equations in this appendix, the following definitions are needed:

$h_I$ = altitude indicated by monitor sensors

$h^*$ = critical altitude

$h_D$ = altitude where fault is detected

$h_{f_j}$ = altitude where jth fault occurs

$\Delta h_I$ = $h_I - h_D$; error in indicated altitude

$p_{f_j}(h_{f_j})$ = probability density function that jth fault occurs at altitude $h_{f_j}$

$p_{D_j}(h_{f_j} - h_D | h_{f_h})$ = conditional probability density function that detection of jth fault is detected at altitude $h_D$ given that the jth fault occurs at altitude $h_{f_j}$

$p_I(\Delta h_I > h^* - h_D)$ = probability that error $\Delta h_I$ is greater than $h^* - h_D$

$p_I(\Delta h_I)$ = probability density function of altitude error $\Delta h_I$

$p_{Dk}(h_D)$ = probability density function that the kth fault is incorrectly identified at altitude $h_D$

$p_{Dk}(h_D | h_{fk})$ = conditional probability density function that the kth fault is identified at altitude $h_D$ given that this fault did not occur at altitude $h_{fk}$

$p_{(f,n)(d,u)(p,a,v)(g,l)(j,k)(c_i | h_D)}$ = failure probability density function

f = fault present in equipment

n = no fault present in equipment

d = primary monitor detected fault

$u$ = primary monitor undetected fault

$p$ = piloted control (displays)

$a$ = automatic control

$v$ = piloted control (visual)

$g$ = go-around decision

$l$ = landing decision

$j$ = index on type of fault (N total)

$k$ = index on type of false fault (N total)

$i$ = index on type of catastrophe (M total)

$p_{fdpgj}(c_i|h_D)$ = conditional probability density function that the ith catastrophe will occur during go-around due to the jth fault being detected at $h_D$

$p_{fdplj}(c_i|h_D)$ = conditional probability density function that the ith catastrophe will occur during landing due to the jth fault being detected at $h_D$

$p_{fualj}(c_i|h_j)$ = conditional probability density function that the ith catastrophe will occur during landing due to the jth fault occuring at $h_{fj}$ and not being subsequently detected

$p_{ndpgk}(c_i|h_D)$ = conditional probability density function that the ith catastrophe will occur during go-around due to the kth fault being incorrectly identified at altitude $h_D$

$p_{ndplk}(c_i|h_D)$ = conditional probability density function that the ith catastrophe will occur during manual landing due to the kth fault being incorrectly identified at altitude $h_D$

$p_{nual}$ = probability of fault-free performance catastrophe

$p_{fual}$ = probability of undetected fault causing automatic landing catastrophe

$p_{fdpg}$ = probability of detected fault causing manual go-around catastrophe

$p_{fdpl}$ = probability of detected fault causing manual landing catastrophe

$p_{ndpg}$ = probability of false fault causing manual go-around catastrophe

$p_{ndpl}$ = probability of false fault causing manual landing catastrophe

$p_{ndvl}$ = probability of false fault causing manual visual landing catastrophe

$p_{fdvl}$ = probability of detected fault causing manual visual landing catastrophe

$h_o$ = altitude at which monitor becomes functional

$P_A$ = probability of catastrophic accident (total system)

$P_{FAE}$ = probability of false primary monitor alarm

$P_{EF}$ = probability of equipment (airborne/ground) fault

$P_{MAE}$ = probability of missed monitor alarm due to primary monitor failure ($P_{MF}$)

$P_D$ = probability of fault detection

$t_1$ = nominal flight duration from $h^*$ to touchdown (TD)

$t_2$ = nominal flight duration from $h_o$ to $h^*$ (critical altitude)

$\alpha_1$ = landing decision exposure factor (Strategy A, B)

$\alpha_2$ = go-around decision exposure factor (Strategy A, B)

$\alpha_3$ = visual landing exposure factor (Strategy B only)

## Mathematical Definitions

Detected Fault Causing Manual Go-Around Catastrophe

$$p_{fdpg} = \sum_{j=1}^{N} \sum_{i=1}^{M} \int_{h_o}^{h^*} \int_{h_o}^{h_D} p_{fdpgj}(c_i | h_D)\ p_I(\Delta h_I > h^* - h_D)$$

$$\cdot\ p_{D_j}(h_{f_j} - h_D | h_{f_j})\ p_{f_j}(h_{f_j}) dh_{f_j}\ dh_D \qquad (10)$$

To compute probability of successful go-around, replace

$$\mathop{\Delta}\limits_{i=1}^{M} p_{fdpgj}(c_i | h_D) \quad \text{by} \quad \left[ 1 - \sum_{i=1}^{M} p_{fdpgj}(c_i | h_D) \right] .$$

Note that in Eq. (A.1)

$$p_I(\Delta h_I > h^* - h_D) = \int_{h_o}^{h^* - h_o} p_I(\Delta h_I)\ dh_I \qquad (11)$$

Detected Fault Causing Manual Landing Catastrophe

$$p_{fdpl} = \sum_{j=1}^{N} \sum_{i=1}^{M} \int_{h^*}^{o} \int_{h_o}^{h_D} p_{fdplj}(c_i | h_D)\ p_I(\Delta h_I < h^* - h_D)$$

$$\cdot\ p_{D_j}(h_{f_j} - h_D\ h_{f_j})\ p_{f_j}(h_{f_j})\ dh_f\ dh_D \qquad (12)$$

To compute the probability of a successful landing, replace

$$\sum_{i=1}^{M} p_{fdplj}(c_i | h_D) \quad \text{by} \quad \left[ 1 - \sum_{i=1}^{M} p_{fdplj}(c_i | h_D) \right] .$$

Probability of a Fault

$$P_E = \sum_{j=1}^{N} \int_{h_o}^{o} p_{f_j}(h_{f_j})\ dh_{f_j} \qquad (13)$$

Undetected Fault Causing Landing Catastrophe

$$P_{fual} = \sum_{j=1}^{N} \sum_{i=1}^{M} \int_{h_o}^{o} \left[ 1 - \int_{h_{f_j}}^{o} p_{D_j}(h_{f_j} - h_D | h_{f_j}) \, dh_D \right] p_{fualj}(c_i | h_{f_j}) \, p_{f_j}(h_{f_j}) \, dh_{f_j} \qquad (14)$$

To compute the probability of a successful landing, replace

$$\sum_{i=1}^{M} p_{fualj}(c_i | h_{f_j}) \quad \text{by} \quad \left[ 1 = \sum_{i=1}^{M} p_{fualj}(c_i | h_{f_j}) \right]$$

Probability of a Missed Alarm

$$P_{MAE} = \Delta_{j=1}^{N} \int_{h_o}^{o} \left[ 1 - \int_{h_{f_j}}^{o} p_{D_j}(h_{f_j} - h_D | h_{f_j}) \, dh_D \right] p_{f_j}(h_{f_j}) dh_{f_j}$$

$$= P_E - P_D \qquad (15)$$

Probability of Detecting a Fault

$$P_D = \sum_{j=1}^{N} \int_{h_o}^{o} \int_{h_{f_j}}^{o} p_{D_j}(h_{f_j} - h_D | h_{f_j}) p_{f_j}(h_{f_j}) dh_D \, dh_{f_j} \qquad (16)$$

Nuisance Disconnect Causing Go-Around Failure

$$P_{ndpg} = \sum_{k=1}^{N} \sum_{i=1}^{M} \int_{h_0}^{h^*} p_{ndpgk}(c_i | h_D) \, p_I(\Delta h_I > h^* - h_D) \cdot p_{D_k}(h_D) dh_D \qquad (17)$$

Here,

$$p_{Dk}(h_D) = \int_{h_o}^{h_D} p_{Dk}(h_D|\bar{h}_{f_k}) \, (1 - p_{f_k}(h_{f_k})) \, dh_{f_k} \tag{18}$$

To compute the probability of a successful go-around, replace

$$\sum_{i=1}^{M} p_{ndpgk}(c_i|h_D) \quad \text{by} \quad \left[1 - \sum_{i=1}^{M} p_{ndpgk}(c_i|h_D)\right]$$

Nuisance Disconnect Causing Landing Failure

$$P_{ndpl} = \sum_{k=1}^{N} \sum_{i=1}^{M} \int_{h^*}^{o} p_{ndplk} \, (c_i|h_D) \, p_I(\Delta h_I < h^* - h_D) \cdot p_{D_k}(h_D) \, dh_D \tag{19}$$

To compute the probability of a successful landing, replace

$$\sum_{i=1}^{M} p_{ndplk}(c_i|h_D) \quad \text{by} \quad \left[1 - \sum_{i=1}^{M} p_{ndplk}(c_i|h_D)\right]$$

Probability of a False Monitor Alarm

$$P_{FAE} = \sum_{k=1}^{N} \int_{h_o}^{o} p_{D_k}(h_D) \, dh_D \tag{20}$$

Computation of Critical Altitude $(h^*)$

When $h \geq h^*$,

$$\sum_{i=1}^{M} \int_{h_o}^{h} \int_{h_o}^{h_D} p_{fdpgj}(c_i|h_D) \, p_I(\Delta h_I > h - h_D) \cdot p_{D_j}(h_{f_j} - h_D|h_{f_j}) \, p_{f_j}(h_{f_j}) \, dh_{f_j} \, dh_D$$

$$\leq \sum_{i=1}^{M} \int_{h}^{o} \int_{h_o}^{h_D} p_{fdplj}(c_i | h_D)\; p_I(\Delta h_I < h - h_D)$$

$$\cdot\; p_{D_j}(h_{f_j} - h_D\; h_{f_j})\; p_{f_j}(h_{f_j})\; dh_f\; dh_D \tag{21}$$

Thus, when $h \geq h^*$, the correct decision is to go-around and for $h < h^*$ it is to land manually.

Exposure Factors for Strategy A

$$\begin{aligned} \alpha_1 &= \frac{T_1}{(T_1 + T_2)} \\ \alpha_2 &= \frac{T_2}{(T_1 + T_2)} \end{aligned} \tag{22}$$

Exposure Factors for Strategy B

$$\begin{aligned} \alpha_1 &= T_1/(T_1 + T_2 + T_3) \\ \alpha_2 &= T_2/(T_1 + T_2 + T_3) \\ \alpha_3 &= T_3/(T_1 + T_2 + T_3) \end{aligned} \tag{23}$$

Probability of Catastrophic Accidents for Design Strategy A

$$\begin{aligned} P_A = \{1 - P_{EF}\}\{P_{nual} + P_{FAE}(\alpha_1\, P_{ndpl} + \alpha_2\, P_{ndpg})\} \\ \cdot\; P_{EF}\{P_{MAE} \cdot P_{fual} + (1 - P_{MAE})(\alpha_1\, P_{fdpl} + \alpha_2\, P_{fdpg})\} \end{aligned} \tag{24}$$

Probability of Catastrophic Accident for Decision Strategy B

$$P_A = \{1 - P_{EF}\}\{P_{nual} + P_{FAE}(\alpha_1 P_{ndpl} + \alpha_2 P_{ndpg} + \alpha_3 P_{ndvl})\} \cdot P_{EF}\{P_{MAE} \cdot P_{fual} + (1 - P_{MAE})(\alpha_1 P_{fdpl} + \alpha_2 P_{fdpg} + \alpha_3 P_{fdvl})\} \tag{25}$$

Independent Landing Monitor (ILM). The incorporation of the ILM into an avionics system with a primary autoland capability, introduces additional terms into the equations, presented in the previous sections. The principal source of these terms is the additional flexibility in the decision making process related to the criterion for initiating a pilot takeover. The four options identified in Table 34 arise due to the potentially conflicting outputs of the primary (i.e., autoland) and secondary (i.e., ILM) monitors.

The equations presented in this section provide a rigorous basis for (a) justifying the incorporation of an ILM, (b) determining the best takeover criterion, and (c) generating performance specifications for the fault detection system.

Table 36.-POST FAULT DETECTION PILOT TAKEOVER CRITERION OPTIONS

| OPTION | TAKEOVER INITIATION CRITERION |
|---|---|
| 1 | Primary monitors only (i.e. no ILM) |
| 2 | ILM or primary monitors |
| 3 | ILM only (i.e. ignore primary monitors) |
| 4 | ILM and primary monitors |

## Probability Definitions

Additional probability terms, introduced by the incorporation of a secondary/ILM monitor are defined in this section.

$P_{FAI}$ = probability of false ILM alarm

$P_{MAS}$ = probability of missed ILM alarm due to ILM failure ($P_{ILM}$) or inherent missed alarm rate ($P_{MAI}$); $P_{MAS} = P_{MAI} + P_{ILM}$

$P_{ELE}$ = probability of emergency landing catastrophe with primary monitors

$P_{GAE}$ = probability of go-around catastrophe with primary monitors

$P_{MLE}$ = probability of manual visual landing catastrophe with primary monitors

$P_{ELI}$ = probability of emergency landing catastrophe with ILM

$P_{GAI}$ = probability of go-around catastrophe with ILM

$P_{MLE}$ = probability of manual landing catastrophe with ILM

$P_{SAE}$ = probability of catastrophe using Strategy A with primary monitors

$P_{SAI}$ = probability of catastrophe using Strategy A with ILM

$P_{SBE}$ = probability of catastrophe using Strategy B with primary monitors

$P_{SBI}$ = probability of catastrophe using Strategy B with ILM

## Mathematical Defintions

### Catastrophe Using Strategy A and Primary Monitors

Defining $P_{ELE} = \max \{P_{ndp1}, P_{fdp1}\}$ , (26)

$$P_{GAE} = \max \{P_{ndpg}, P_{fdpg}\} \qquad (27)$$

we get
$$P_{SAE} = \alpha_1 P_{ELE} + \alpha_2 P_{GAE} \qquad (28)$$

Catastrophe Using Strategy B and Primary Monitors

Defining
$$P_{MLE} = \max \{P_{ndvl}, P_{fdvl}\} \qquad (29)$$

we get
$$P_{SBE} \cong \alpha_1 P_{ELE} + \alpha_2 P_{GAE} + \alpha_3 P_{MLE} \qquad (30)$$

Catastrophe Using Strategy A and ILM

Defining
$$P_{ELI} = \max \{P_{ndpl}, P_{fdpl}\}_I \qquad (31)$$

$$P_{GAI} \cong \max \{P_{ndpg}, P_{fdpg}\}_I \qquad (32)$$

we get
$$P_{SAI} \cong \alpha_1 P_{ELI} + \alpha_2 P_{GAI} \qquad (33)$$

where the subscript I denotes usage of an ILM. Note that the performance of the system can potentially be improved during emergency landing (EL) and go-around (GA) by using guidance commands supplied by the ILM.

Catastrophe Using Strategy B and ILM

Define
$$P_{MLI} = \max \{P_{ndvl}, P_{fdvl}\}_I \qquad (34)$$

where subscript I denotes usage of an ILM. Note that in this case the ILM sensor must provide visibility enhancement. This gives the result

$$P_{SBI} = \alpha_1 P_{ELI} + \alpha_2 P_{GAI} + \alpha_3 P_{MLI} \qquad (35)$$

# APPENDIX B
# COVARIANCE PROPAGATION ANALYSIS

The assessment of post fault recovery performance is made by conducting a covariance propagation analysis. The objective of this appendix is to (1) describe the mathematical models used for the aircraft/display/pilot system, (2) present the covariance propagation equation, and (3) relate the time sequence of covariance matrices to the catastrophic failure probabilities defined in Appendix A.

The closed loop pilot display aircraft block diagram is shown in Figure 36; the blocks in this figure are described in the following.

## Linearized Aircraft Model (B-737)

Linearized longitudinal and lateral axis models of the Terminally Configured Vehicle (B-737) were developed to conduct the covariance propagation analysis. The linearized aircraft equations are described by the vector differential equation,

$$\dot{x} = Fx + Gu + \Gamma_d w_d \tag{36}$$

where x is the state vector, u is the control input vector, and $w_d$ is the disturbance vector. It is assumed that $w_d$ is a zero mean white noise source with

$$E\{ w_d w_d^T \} = Q \tag{37}$$

The longitudinal and lateral decoupled perturbation equations are numerically specified in Figures 37 and 38, respectively, for the flight condition.

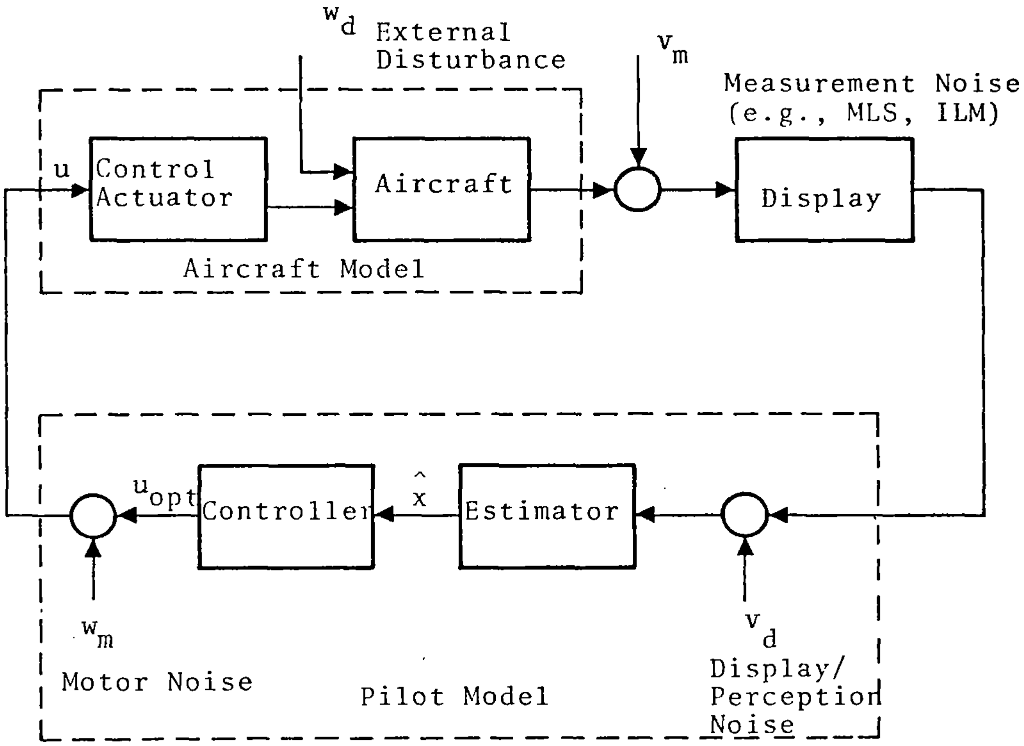


FIGURE 36 .-MANUAL CONTROL SYSTEM BLOCK DIAGRAM

$$
\begin{bmatrix} \dot{\theta} \\ \dot{u} \\ \dot{\alpha} \\ \dot{q} \\ \dot{h} \\ \dot{R}_s \end{bmatrix}
=
\begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 0 \\
-0.1563 & 0.0464 & 0.018 & 0 & 0 & 0 \\
0.0083 & -0.315 & 0.58 & -0.9998 & 0 & 0 \\
-0.00036 & 0.0169 & 1.03 & 0.458 & 0 & 0 \\
200 & 8.2 & 0 & 0 & 0 & 0 \\
0 & 205 & 0 & 0 & 0 & 0
\end{bmatrix}
\bullet
\begin{bmatrix} \theta \\ u \\ \alpha \\ q \\ h \\ R_s \end{bmatrix}
+
$$

$$
\begin{bmatrix}
-0 & 0 \\
0 & 0.0017 \\
-0.0393 & -0.000166 \\
-1.01 & 0.00572 \\
0 & 0 \\
0 & 0
\end{bmatrix}
\bullet
\begin{bmatrix} \delta_e \\ \delta_T \end{bmatrix}
+
\begin{bmatrix}
0 & 0 \\
-0.0464 & 0.081 \\
-0.315 & -0.587 \\
0.619 & -0.103 \\
0 & 0 \\
0 & 0
\end{bmatrix}
\bullet
\begin{bmatrix} u_g \\ \alpha_g \end{bmatrix}
$$

$\theta$ = pitch
u = normalized velocity
$\alpha$ = angle-of-attack
q = pitch rate
h = altitude
$R_s$= slant range

$\delta_e$ = elevator
$\delta_T$ = thrust

$u_g$ = gust component (longitudinal)
$\alpha_g$ = gust component (angle-of-attack)

FIGURE 37.-LONGITUDINAL PERTURBATION EQUATIONS

$$\begin{bmatrix} \dot{\phi} \\ \dot{\psi} \\ \dot{\beta} \\ \dot{p} \\ \dot{r} \\ \dot{L} \end{bmatrix} = \begin{bmatrix} \theta & 0 & 0 & -0.0524 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0.1563 & 0 & -0.13 & -0.996 & 0 \\ 0 & 0 & -3.18 & 1.1 & 0 \\ 0 & 0 & 1.04 & -0.215 & 0 \\ 0 & 200 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} \phi \\ \psi \\ \beta \\ p \\ r \\ L \end{bmatrix} +$$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.00862 & 0.356 \\ 2.58 & 0.538 \\ 0.1008 & -0.0678 \\ 0 & \end{bmatrix} \cdot \begin{bmatrix} \delta_a \\ \delta_r \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ -0.13 \\ -3.8 \\ 1.04 \\ 0 \end{bmatrix} \beta_g$$

$\phi$ = roll angle
$\psi$ = yaw angle
$\beta$ = sideslip angle
$p$ = roll rate
$r$ = yaw rate
$L$ = Lateral Displacement

$\delta_a$ = aileron
$\delta_r$ = rudder

$\beta_g$ = gust componenet (sideslip)

FIGURE 38.- LATERAL PERTURBATION EQUATIONS

| | |
|---|---|
| Altitude | = 305m (1000 ft) |
| Airspeed | = 120 kts |
| Weight | = 31,800 kg (70,000 lb) |
| Thrust | = 38,440 Nt (8654 lb) |
| Angle-of-Attack | = 4.37° |
| Flight Path Angle | = -3° |

For the longitudinal axis, the go-around maneuver was simulatd by open loop commands for the elevator and thrust inputs given by:

$$\delta_e(t) = \delta_{e_0} + \dot{\delta}_{e_{max}} (t-t_0) \qquad (38)$$

where

$\delta_e \leq \delta_{e_{max}}$ = (maximum elevator angle)

$\dot{\delta}_{e_{max}}$ = maximum elevator rate

$\delta_{e_0}$ = elevator command at $t = t_0$

and

$$\delta_{Th}(t) = \delta_{Th\ max} + [\delta_{Th0} - \delta_{Th\ max}]e^{-t/\tau} \qquad (39)$$

where

$\delta_{Th}$ max = 62,150 Nt (14,000 lb)

$\tau$ = 1 s

$\delta_{Th_0}$ = thrust command at $t = t_0$

In addition, the angle-of-attack was constrained during the maneuver by appropriately limiting the thrust $\delta_{th}(t)$ and elevator $\delta_e(t)$, so that

$$\alpha(t) \leq \alpha_{max} \tag{40}$$

where $\alpha_{max} = 18°$

### Display (Measurement) Equation

The display system in Figure 36, represented by the equation,

$$z = Hx + v \tag{41}$$

where the measurement matrix H is defined in Figure 39 for the longitudinal and lateral axis. The noise V, made up of measurement noise $v_m$ and display noise $V_d$, is defined by

$$v = Hv_m + v_d \tag{42}$$

It is assumed that v is a zero mean, white noise source with

$$E\{vv^T\} = R \tag{43}$$

### Pilot Model

A number of math models have been proposed to characterize the pilot in the glideslope and localizer tracking phase of the manual landing task. These models range from the frequency domain transfer function to the optimal control models.

LONGITUDINAL:

$$\begin{bmatrix} \theta_m \\ u_m \\ \alpha_m \\ h_m \\ R_s \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \theta \\ u \\ \alpha \\ q \\ h \\ R_s \end{bmatrix} + v$$

LATERAL:

$$\begin{bmatrix} \phi_m \\ \psi_m \\ \beta_m \\ L_m \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \phi \\ \psi \\ \beta \\ p \\ r \\ L \end{bmatrix} + v$$

FIGURE 39.-DISPLAY (MEASUREMENT) EQUATION

An isomorphic form for the optimal control model was proposed by Kleinman [33], as shown in Figure 40. This model attempts to retain a one-to-one correspondance with hypothesized pilot activity, in terms of an observation phase, information processing phase and a motor phase. From an input-output point of view, this model can be simplified to that in Figure 41. Although neither of these models has been fully validated, analysis to date indicates that the latter model, consisting of a Kalman estimator followed by an optimal controller is an adequate representation for currently available pilot data.

To incorporate the motor noise term into the aircraft equations as in Figure 36, define

$$u(t) = u_{opt} + w_m \qquad (44)$$

The aircraft equation is augmented so that

$$\dot{x} = Fx + Gu_{opt} + \Gamma w \qquad (45)$$

where

$$\Gamma = \left[\begin{array}{c|c} \Gamma_d & 0 \\ \hline 0 & G \end{array}\right] \qquad (46)$$

$$w = \left[\begin{array}{c} w_d \\ \hline w_m \end{array}\right] \qquad (47)$$

and

$$Q = E\{ww^T\} \qquad (48)$$

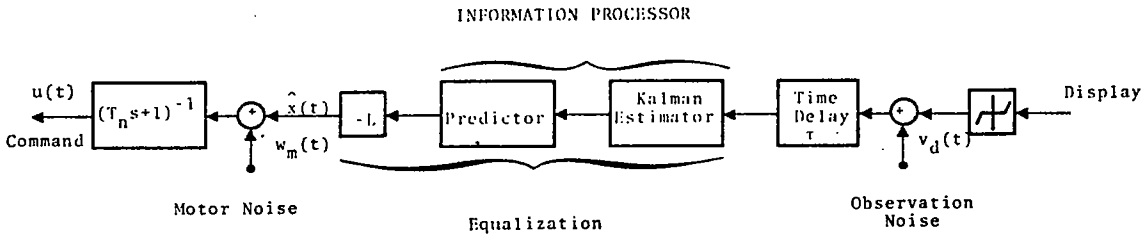


FIGURE 40.-OPTIMAL CONTROL MODEL OF PILOT RESPONSE

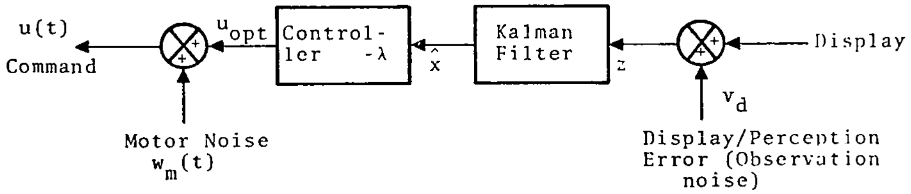


FIGURE 41.-SIMPLIFIED PILOT MODEL

Referring to Figure 36, the objective of the pilot, during the tracking task is to keep deviations from the nominal path as small as possible, using the feedback control u(t). Note that the equations (36) and (45) are linearized perturbation equations and do not include the nominal trajectory. Similarly the control input u(t), only represents the corrective part of the control action and includes the open loop nominal commands.

Thus, the objective of the pilot, as an optimal controller is to minimize a quadratic index of the form.

$$J = 1/2\int_0^T (x^TAx + u^TBu)\ dt \qquad (49)$$

For computational efficiency, if the steady state assumption is made (i.e., $T \rightarrow \infty$ ), then the filter and controller gains are time invarient. But the filter representing the pilot is no longer optimal. Moreover the state estimate and state estimation errors are correlated. As a consequence the covariance propagation analysis, described in the next section, must be performed with the augmented state vector $\{ x \,\vdots\, \hat{x}\}^T$ , where $\hat{x}$ is the state estimate of the "infinite time" version of the Kalman estimator.

The numerical values of the weighting matrices A and B, and the process and measurement noise terms Q and R, are presented in Figure 42

## Covariance Propagation

Based on the pilot-aircraft-display model described above, the objective of this section is to define the equations used to assess post fault detection recovery performance.

The initial state covariance matrix $P^*(0)$ represents the envelope of dispersions of the aircraft state x at the point of fault detection. The covariance propagation technique

LONGITUDINAL:

$A = \text{diag}\ [33, 100, 33, 0, 0.01, 0.001]$

$B = \text{diag}\ [130, 0.25]$

$Q = \text{diag}\ [0.01, 0.0025]$

$R = \text{diag}\ [0.0003, 0.000068, 0.0003, 1, 25]$

LATERAL:

$A = \text{diag}\ [33, 33, 33, 0, 0, 10^{-6}]$

$B = \text{diag}\ [13, 33]$

$Q = 10^{-10}$

$R = \text{diag}\ [0.00015, 0.00015, 0.00015, 12.5]$

FIGURE 42.-NUMERICAL VALUES FOR PILOT MODEL AND PROCESS-MEASUREMENT NOISE COVARIANCES

is used to determine the manner in which the covariance matrix P* evolves from P*(0). This matrix finally reaches the steady state nominal value (due to external disturbances only).

To perform covariance propagation, define an augmented system vector differential equation of dimension 2n,

$$\begin{bmatrix}\dot{x}\\ \hat{x}\end{bmatrix} = \left[\begin{array}{c|c} F & -G\lambda \\ \hline KH & F-G\lambda-KH \end{array}\right] \begin{bmatrix}x\\ \hat{x}\end{bmatrix} + \left[\begin{array}{c|c} \Gamma & 0 \\ \hline 0 & K \end{array}\right] \begin{bmatrix}W\\ V\end{bmatrix} \qquad (50)$$

Define

$$P^* = E\left\{\begin{bmatrix}x\\ \hat{x}\end{bmatrix}[x \quad \hat{x}]^T\right\} + \left[\begin{array}{c|c} P_{11}^* & P_{12}^* \\ \hline P_{21}^* & P_{22}^* \end{array}\right]_{2n \times 2n} \qquad (51)$$

and

$$F^* = \left[\begin{array}{c|c} F & -G\lambda \\ \hline KH & K-G\lambda-KH \end{array}\right] \qquad (52)$$

Then the vector differential equation to propagate the initial covariance is,

$$\dot{P}^* = F^*P^* + P^*F^{*T} + \left[\begin{array}{c|c} \Gamma W \Gamma^T & 0 \\ \hline 0 & KRK^T \end{array}\right] \tag{53}$$

The initial covariance matrix $P^*(0)$, at the point of fault detection, is

$$P^*(0) = \left[\begin{array}{c|c} P^*_{11}(0) & 0 \\ \hline 0 & P^*_{11}(0) \end{array}\right] \tag{54}$$

Thus, to evaluate fault recovery performance, Equation (53) is numerically integrated for the longitudinal and lateral representations of the system. To determine whether the resulting time sequence of covariance matrices represent a "successful" post fault detection recovery, it is necessary to relate the covariance matrix to the probability of catastrophe, during a landing or go-around maneuver defined in Appendix A; this is discussed in the next section.

## Computation of Catastrophe Probability From The Covariance Matrix

The system fault recovery performance is evaluated by starting with an initial covariance matrix (representing the state of the aircraft at fault detection, in a statistical sense). Then, by performing covariance propagation, the time sequence by which this initial covariance transitions to the nominal covariance matrix, (by the stable pilot/display/aircraft feedback control system) is obtained. This is graphically depicted for the landing/go-around task, for one of the system states (altitude), in Figures 43a and 43b, respectively. The following discussion relates the probability of catastrophe resulting from a go-around ($P_{GAE}$/

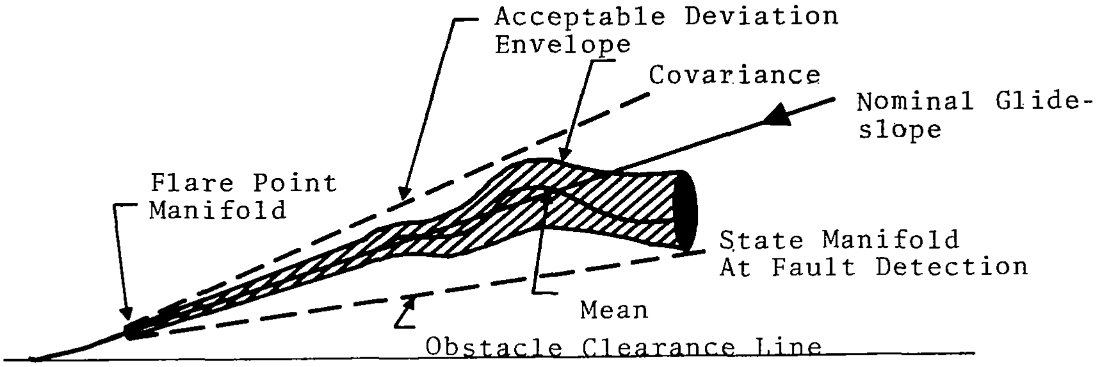


FIGURE 43a.-MANUAL LANDING TASK FAULT RECOVERY

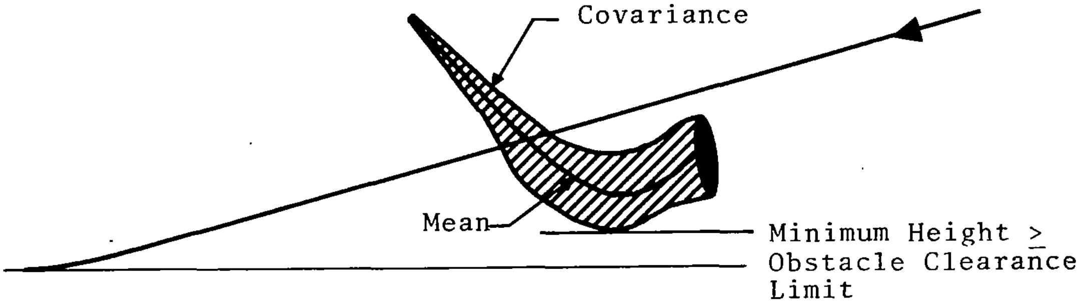


FIGURE 43b.-MANUAL GO-AROUND TASK FAULT RECOVERY

$P_{GAI}$) and landing ($P_{MLE}/P_{MLI}$), defined in Appendix A and used in Chapter III, to the covariance propagation computations.

Let x be the random n-vector representing the system state whose components can take on a continuous set of values with the probability density function

$$p(x) = \frac{1}{(2\pi)^{n/2}|P|^{1/2}} \exp\left[-1/2\ (x-\bar{x})^T P^{-1}(x-\bar{x})\right] \qquad (55)$$

where

$$E(x) = \bar{x} = \text{mean value of state vector} \qquad (56)$$

and

$$E\{(x-x)\ (x-x)^T\} = P = \text{covariance matrix of vector} \qquad (57)$$

It is of interest to determine the constant '$\ell$' such that the probability that x lies outside the hyperellipsoid.

$$(x-\bar{x})^T P^{-1}(x-\bar{x}) = \ell^2 \qquad (58)$$

is less than the go-around ($P_{GAE}/P_{GAI}$) or landing ($P_{MLE}/p_{MLI}$) catastrophe probability requirement. Then, an approximate method of ensuring that the hyperellipsoid defined by Equation (58) does not violate any of the state constraints (e.g., angle-of-attack, obstacle clearance, etc.), is to check whether inequalities of the form,

$$|x_i \pm \ell\sigma_i| < x_{i\ max},\ i = 1, \ldots n. \qquad (59)$$

where $x_{i\,max}$ is the maximum allowable deviation in state i and $\sigma_i^{\ 2}$ is the $i_{th}$ diagonal element of the covariance matrix.

A more accurate method of ensuring constraint satisfaction is to define the constraint boundaries as another hyperellipsoid of the form,

$$(x-\overline{x})^T C(x-\overline{x}) \leq m^2 \tag{60}$$

Then it can be shown that the necessary and sufficient condition for constraint satisfaction is the matrix,

$$\left\{\left(\frac{C}{m^2}\right) - \left(\frac{P^{-1}}{\ell^2}\right)\right\} \geq 0 \tag{61}$$

i.e., the matrix defined by Eq. (61) is positive semidefinite. For the purposes of the present study, inequalities of the form of Eq. (59) were checked. The evaluation of catastrophe probability as a function of n and ℓ was performed and is tabulated in Table 37. It can be seen that for a sixth order system to achieve a probability of catastrophic accident of about $10^{-4}$ (e.g., required for go-around and landing in Appendix A), the four sigma (4σ) covariance dispersion boundary must be checked for constraint violation. The assumed aircraft recovery limits and the flare point window are presented in Table 36 . The recovery is considered to be "successful" if the recovery limits are not included and the "time-to-correct" is that required to satisfy the flare point window constraints of Table 36.

## Extension of the Covariance Propagation Technique

The previous sections described the manner in which the covariance propagation technique, together with certain probability integrals, allow one to evaluate the system fault recovery performance. This methodology was applied to the specific numerical example documented in Figures 37 and 38 , for the flight condition noted in the appendix earlier. To perform the analysis more thoroughly, it is essential that the entire flight trajectory be considered. The conceptual framework by which this is accomplished is now discussed.

Consider a typical terminal area trajectory depicted in Figure 44 (also described in Chapter II). The different flight phases during the traversal of this trajectory are partitioned in the figure and are labeled a, b, c, d, and e. When the aircraft is flying along this trajectory, using the primary autoland system, each of these phases can be mathematically characterized by a linear perturbation equation such as Eq. (36), with the feedback loop shown in Figure 36 being closed by the autoland system. Table 39 shows the sequence of system matrices, together with the corresponding autoland estimator, controller and cost function. Similarly, Table 40 depicts the same sequence of matrices when the system is under manual control.

TABLE 37 -CATASTROPHE PROBABILITIES AS A FUNCTION OF SYSTEM DIMENSIONALITY(n) AND MULTIPLE ($\ell$) OF STANDARD DEVIATION($\sigma$)

| $\ell$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| n | (x $10^{-4}$) | (x $10^{-6}$) | (x $10^{-8}$) | (x $10^{-10}$) | (x $10^{-12}$) |
| 4 | 0.3 | 0.5 | 0.3 | 0.06 | 0.001 |
| 5 | 0.68 | 1.4 | 1.0 | 0.22 | 0.01 |
| 6 | 1.3 | 3.4 | 2.8 | 0.75 | 0.1 |
| 7 | 2.5 | 7.6 | 7.3 | 2.27 | 0.2 |
| 8 | 4.2 | 15.6 | 17.6 | 6.36 | 0.8 |

TABLE 38.-ASSUMED AIRCRAFT RECOVERY LIMITS AND FLARE POINT WINDOW

| STATE | RECOVERY LIMITS |  | FLARE POINT WINDOW | AXIS |
|---|---|---|---|---|
|  | MAX | MIN |  |  |
| θ, ° | 12 | - 12 | ± 0.5 | Longitudinal |
| u, - | 0.15 | - 0.15 | ± 0.02 |  |
| α, ° | + 22 | - 10 | ± 0.5 |  |
| q, °/s | 3 | - 3 | ± 0.05 |  |
| h, m(ft) | 305(100) | - 30.5(-100) | ± 1.5(± 5) |  |
| $R_s$,m(ft) | 915(3000) | -610(-2000) | ± 3.05(±10) |  |
| $\delta_e$, ° | 10 | - 5 | ± 1 |  |
| $\delta_{th}$ | 5000 | -500 | ± 100 |  |
| ϕ, ° | 15 | - 15 | ± 1 | Lateral |
| ψ, ° | 15 | - 15 | ± 1.5 |  |
| β, ° | 5 | - 5 | ± 1.5 |  |
| p, °/s | 5 | - 5 | ± 0.5 |  |
| r, °/s | 5 | - 5 | ± 0.5 |  |
| L,m(ft) | 152(500) | -152(-500) | ± 6.1(±20) |  |

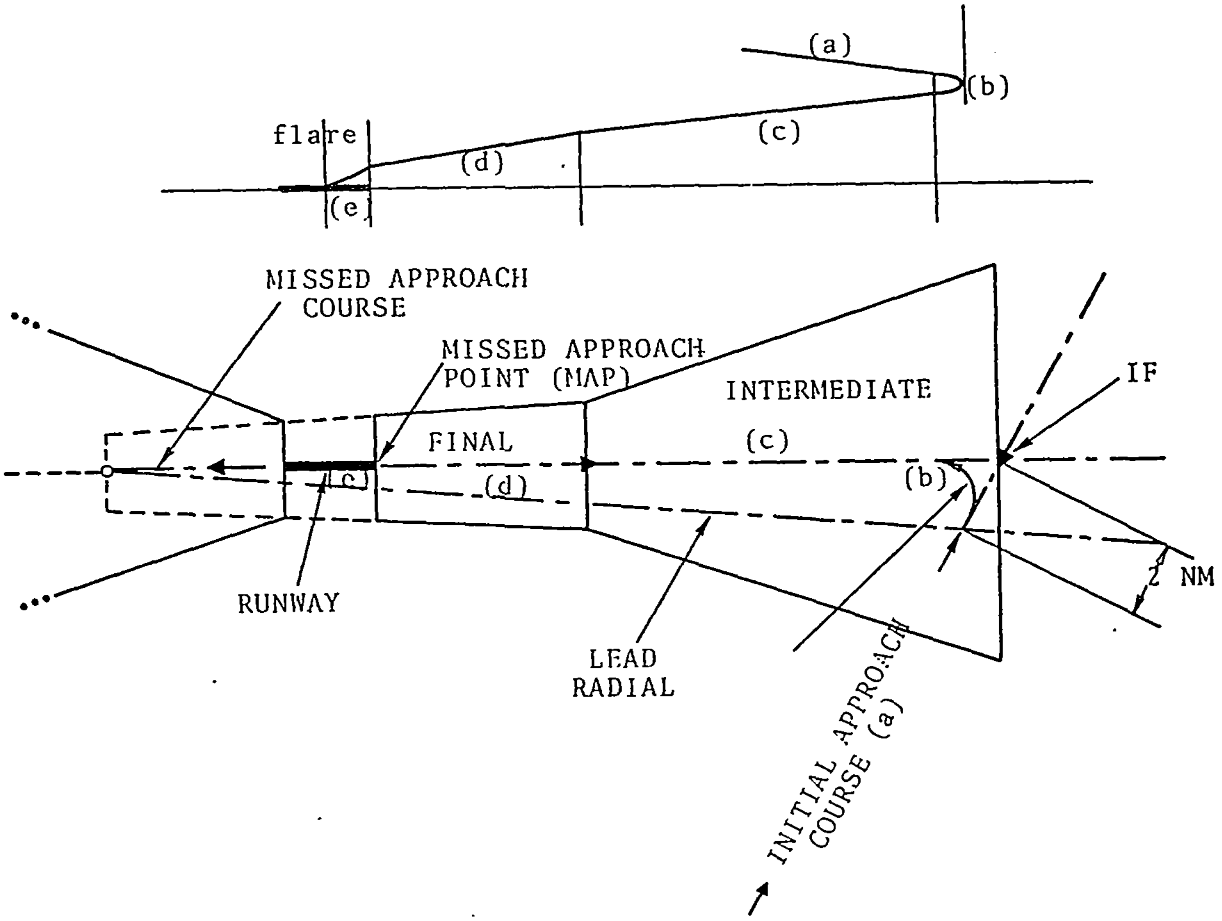


FIGURE 44.-TYPICAL TERMINAL AREA TRAJECTORY

TABLE 39.-MATHEMATICAL DESCRIPTION OF NOMINAL AUTOLAND (PRIMARY SYSTEM) FLIGHT PHASES

| PHASE | SYSTEM MATRICES | AUTOLAND MODEL | | AUTOLAND COST FUNCTION | COMMENTS |
|---|---|---|---|---|---|
| | | ESTIMATOR | CONTROLLER | | |
| a | $F_{aa}, G_{aa}$ | $K_{aa}$ | $\lambda_{aa}$ | $A_{aa}, B_{aa}$ | Approach flaps, gear down, loose tracking |
| b | $F_{ab}, G_{ab}$ | $K_{ab}$ | $\lambda_{ab}$ | $A_{ab}, B_{ab}$ | Curved, descending |
| c | $F_{ac}, G_{ac}$ | $K_{ac}$ | $\lambda_{ac}$ | $A_{ac}, B_{ac}$ | GS = 5°, landing flaps, decelerating |
| d | $F_{ad}, G_{ad}$ | $K_{ad}$ | $\lambda_{ad}$ | $A_{ad}, B_{ad}$ | GS = 2.8°, tight tracking |
| e | $F_{ae}, G_{ae}$ | $K_{ae}$ | $\lambda_{ae}$ | $A_{ae}, B_{ae}$ | Flare |

*Nomenclature:* $A_{(a|m|F)}$ (a . . . e)

First Subscript (a|m|F): Automatic/Manual Fault

Second Subscript (a . . . e): Flight Phases

TABLE 40.-MATHEMATICAL DESCRIPTION OF NOMINAL MANUAL CONTROL (BACKUP SYSTEM) FLIGHT PHASES

| PHASE | SYSTEM MATRICES | PILOT MODEL |  | FUNCTION | COMMENTS |
|---|---|---|---|---|---|
|  |  | ESTIMATOR | CONTROLLER |  |  |
| a | $F_{ma}, G_{ma}$ | $K_{ma}$ | ma | $A_{ma}, B_{ma}$ | Approach flaps, gear down, loose tracking |
| b | $F_{mb}, G_{mb}$ | $K_{mb}$ | mb | $A_{mb}, B_{mb}$ | Curved, descending |
| c | $F_{mc}, G_{mc}$ | $K_{mc}$ | mc | $A_{mc}, B_{mc}$ | GS = 5°, landing flaps, decelerating |
| d | $F_{md}, G_{md}$ | $K_{md}$ | md | $A_{md}, B_{md}$ | GS = 2.8°, tight tracking |
| e | $F_{me}, G_{me}$ | $K_{me}$ | me | $A_{me}, B_{me}$ | Flare |

Thus, to thoroughly evaluate the overall system performance, linear perturbation models must be constructed for each of these phases, and the covariance propagation program must be exercised to sequence through the entire trajectory.

Two flight phases are singled out for further comment, namely, flare and go-around. During the flare phase, the system model is essentially nonlinear due to the flare control law and the ground effect on aerodynamic coefficients. Consequently, a sequence of models rather than a single model is needed to represent this phase. For go-around, the aircraft controls are at their limiting values, and again, a sequence of models is necessary to describe accurately the transition from small signal perturbations to a limiting control situation.

# APPENDIX C

## STATISTICAL TESTS

Depending on the hypothesis being tested, a number of statistical tests can be used [22-25]. The applicable tests, to detect changes in the mean and variance, are presented in Table 41. This table categorizes the statistical tests according to the hypothesis and whether the sample is univariate or multivariate. Let $\{x_i\}_{i=1}^{n}$ be a sample from a normal distribution with constant mean $\mu_o$ and variance $\sigma_o^2$. To test whether a given sample $\{x_i\}$ satisfies the null hypothesis $(\sigma^2 = \sigma_o^2)$ or the alternate $(\sigma^2 \neq \sigma_o^2)$ one can perform either a likelihood ratio test [22] or a chi square $(\chi^2)$ test. Even under the assumption of normality and independent sample assumption, the likelihood ratio test is a complex function of the sample variance. Analytical or empirical results on the distribution of the likelihood ratio tests, necessary to compute test thresholds, are not available in literature. Therefore, in practice, a chi square $(\chi^2)$ test from the null hypothesis (denoted by $H : \sigma = \sigma_o^2$) is used. This test is also used here, for detecting univariate variance changes as documented in Table 41.

The statistic for the $\chi^2$ test is

$$\chi^2 = \frac{(n-1)\ s^2}{\sigma_o^2} \tag{62}$$

which under $H_o$ has a $\chi^2$ distribution with $\nu = n-1$ degrees of freedom.

The usual central region is thus made up of

$$s^2 < \{\sigma_o^2\ \chi^2_{\eta/2}\ (n-1)\}/(n-1) \tag{63}$$

and

$$s^2 > \{\sigma_o^2\ \chi^2_{1-\eta/2}\ (n-1)\}/(n-1) \tag{64}$$

where

## TABLE 41.-APPLICABLE PARAMETRIC STATISTICAL TESTS

| HYPOTHESES | UNIVARIATE | | MULTIVARIATE (ONE-SIDED NOT APPLICABLE) | |
|---|---|---|---|---|
| MEAN | σ KNOWN | σ UNKNOWN | σ KNOWN | σ UNKNOWN |
| $H_o: \mu = \mu_o$<br>$H_1: \mu \neq \mu_o$ | Z TEST:<br>$Z_o = \frac{1}{2} \log \frac{1+r}{1-r}$<br>r: CORRELATION COEFFICIENT (BI-VARIATE) | t TEST:<br>$t_o = \frac{(\overline{X}-\mu_o)}{S}\sqrt{n}$<br>ROBUST TO NORMALITY ASSUMPTION<br>$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$ | $\chi^2$ TEST<br>(VECTOR CASE) | $T^2$ TEST:<br>$T^2 = N(\overline{X}-\mu_o)^T, S^{-1}(\overline{X}-\mu_o)$<br>$T^2 = (N-1) (\lambda_o^{-2/N} - 1)$<br>S = COVARIANCE MATRIX<br>$\lambda_o$ = CONFIDENCE LEVEL SETTING |
| VARIANCE<br>$H_o: \sigma^2=\sigma_o^2$<br>$H_1: \sigma^2\neq\sigma_o^2$<br>$\sigma^2>\sigma_o^2$ | MAXIMUM LIKELIHOOD TEST<br>LARGE SAMPLE APPROXIMATION: $\chi^2$<br>μ KNOWN/UNKNOWN<br>$\chi_o^2 = \frac{(n-1)S^2}{\sigma_o^2}$ ; $S^2=\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\overline{X})^2$<br>NOT ROBUST TO NORMALITY ASSUMPTION | | MAXIMUM LIKELIHOOD TEST<br>LARGE SAMPLE APPROXIMATION: $T^2$<br>μ KNOWN/UNKNOWN | |

$$s^2 = \left(\frac{1}{n-1}\right) \sum_{i=1}^{n} (x_i - \overline{x})^2 \qquad \text{sample variance} \qquad (65)$$

$$\overline{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \qquad \text{sample mean} \qquad (66)$$

and $\eta$ = false alarm rate.

For one sided tests with the alternate hypothesis $\sigma^2 > \sigma_o^2$, the central region is

$$s^2 > \{\sigma_o^2 \chi_{1-\eta}^2 (n-1)\}/(n-1) \qquad (67)$$

A 100(1-$\eta$)% confidence interval for $\sigma^2$ is

$$(n-1)s^2/\chi_{1-\eta/2}^2(n-1) < \sigma^2 < \frac{(n-1)s^2}{\chi_{\eta/2}^2(n-1)} \qquad (68)$$

The probability, P, depends on the alternate hypothesis. For example, if the alternate hypothesis is $\{H_1: \sigma > \sigma_o^2\}$ then,

$$P = \Pr\{\chi^2(n-1) > \chi_o^2\} \qquad (69)$$

However real sample data $\{x_i\}$ are usually correlated. Since the $\chi^2$ test assumes random samples, the test results will be degraded. In other words, probability of false alarm $\eta$ will in general be larger than the value assumed in the calculations preceding this test. An empirical study needs to be conducted to evaluate the effects of departures from the underlying assumptions.

Another source of error includes deviations from the assumption of normality. The chi-square test is not robust with respect to the normality assumption. Sensitivity of the test to deviations from normality can be studied empirically.

To test the hypothesis that the mean $\mu$ is equal to some constant $\mu_o$ (denoted by $H_o$: $\mu = \mu_o$), the t test is used when

$\sigma^2$ is unknown. The t test statistic is [24]

$$t_o = \frac{(\bar{x} - \mu_o)}{s} \sqrt{n} \tag{70}$$

which under $H_o$ has a student's t distribution with $\nu = n-1$ degrees of freedom. As in the $\chi^2$ test, the P value depends on the alternate hypothesis. When the alternate hypothesis is $\{H_1: \mu \neq \mu_o\}$, then

$$P = 2\Pr\{t(\nu) > |t_o|\} \tag{71}$$

An interval estimate for $\mu$ is given by the $100(1-\eta)\%$ confidence interval

$$x - t_{1-(\eta/2)}(n-1) \quad s/\sqrt{n}, \quad x + t_{1-(\eta/2)}(n-1) \quad s/\sqrt{n} \tag{72}$$

where $t_{1-(\eta/2)}(n-1)$ is the $100[1-(\eta/2)]$th percentile of the student's t distribution with $\nu = n-1$ degrees of freedom. This interval is used to test $\{H_o: \mu = \mu_o\}$ against $\{H_1: \mu \neq \mu_o\}$. $H_0$ is rejected at level $\eta$ if $\mu_0$ falls outside this confidence interval. Unlike the $\chi^2$ test, the t test is known to be robust, that is, insensitive to moderate deviations from the assumption of normality, when the sample is random.

# REFERENCES

1. Cortright, E.M., "Program Plan for Terminally Configured Vehicle Program," NASA Langley, December 1971.

2. Anon., "Study to Determine and Assess Information and Display Requirements for Potential ILM Systems," NASA RFP-1-14-4500, January 1974.

3. Anon., "Engineering and Development Program Plan - All Weather Landing," Report No. FAA-ED-07-3, October 1972.

4. Anon., "All Weather Landing Systems Program," FAA-RFP-WA5S-4-0288, May 1974.

5. Anon., "MLS Technique Assessment," MLS Working Group, Radio Technical Committee on Aeronautics, December 1974.

6. Conn, R., et al., "Definition and Tradeoff Study of Reconfigurable Airborne Digital Computer System Organization," NASA-CR-132537, November 1974.

7. "Automatic Landing Systems (ALS)," FAA Advisory Circular, AC No. 20-57A, January 1971.

8. Hooker, D., et al., "Survivable Flight Control Systems: Studies, Analysis and Approach," McDonnell-Douglas, AD 733582, May 1971.

9. Shah, N.M., et al., "The Effect of Aircraft Environment on Category III Autoland Performance and Safety," AIAA Paper 72-811, Aircraft Design, Flight Test, and Operations Meeting, Los Angeles, California, August 1972.

10. Gorham, J.A., "Automatic Flight Control and Navigation Systems on the L-1011 - Capabilities and Experiences," USSR/US Aeronautical Technology Symposium, Moscow, July 1973.

11. Anon., "International Standards and Recommended Practices," International Civil Aviation Organization (ICAO), Annex 10, Annex 14, April 1968; Amendment 49, January 1972.

12. Anon., "United States Standard for Terminal Instrument Procedures (TERPS)," FAA Handbook 8260.3A, February 1970; Chg. 1, August 1970; Chg. 2, May 1972.

13. Anon., "Criteria for Approving Category I and Category II Landing Minima for FAR 121 Operations," FAA Advisory Circular, AC No. 120-29, September 1970; Chg. 1, December 1971; Chg. 2, July 1972.

14. Anon., "C-141 Category III All Weather Landing System, Vol. 1: Results of Flight Testing," Lockheed-Georgia, Report. No. ER8206, August 1968.

15. Anon., "Criteria for Approval of Category IIIA Landing Weather Minimums," FAA Advisory Circular, AC No. 120-28A, December 1971.

16. Russel, W., "From Automatic Landing to Category III," SAE Paper No. 710441, National Air Transportation Meeting, Atlanta, May 1971.

17. Holliday, G. and Gorham, J.A., "Development Testing of the L-1011 Independent Landing Monitor," SAE No. 710433, National Air Transportation Meeting, Atlanta, May 1971.

18. Jester, D.L., et al., "Implementation of the DC-10 Performance and Failure Assessment Monitor," Douglas Aircraft Co., Report No. MDC-J4121D, March 1971.

19. Parks, D.L. and Tubb, D.G., "Simulator Development of a Perspective Display as an Independent Landing Monitor," AIAA Paper 70-924, Los Angeles, California, July 1970.

20. Smith, J.M., at al., "Principles of Performance Monitoring with Application to Automatic Landing," J. of Aircraft, Vol. 9, No. 5, May 1972, pp. 339-346.

21. Parks, D.L., et al., "Development of an Independent Altitude Monitor Concept," Report No. FAA-RD-168, September 1973.

22. Wempe, T. and Palmer, E., "Pilor Performance With a Simulated Pictorial Landing Display Including Different Conditions of Resolution and Update Rate," Sixth Annual Conference on Manual Control, Wright-Patterson AFB, Ohio, April 1970.

23. Bobbett, E.M. and Woodruff, K.R., "Rate-of-Closure as a Performance Monitoring Parameter," AGARD-CP-96-71, Guidance, Control and Display Conference, Paper 22-1, 1971.

24. Shrager, J.J., "Advanced Flight Control and Electronic Display Systems for All-Weather Flight Operation: A Literature Review and Bibliography," Report No. FAA-EM-74-12, June 1974.

25. Anon., "Analytical Evaluation of Various Potential Sensors for Use in an Independent Landing Monitor (ILM) for Conventional Takeoff and Landing (CTOL) Aircraft," NASA-RFP-1-14-4534, February 1974.

26. DeCelles, J.L., et al., "A Rational Program for Low Visibility Landing," NTSB Approach and Landing Accident Forum, October 1972.

27. Harenberg, H.L. and Shannon, J.H., "Development of the DC-10 Automatic Landing Monitor, McDonnell-Douglas Corp., 1973.

28. Anon., "Principles of Monitoring Aeronautical Ground Electronics Facilities," RTCA-DO-133,

29. Brownlee, K.A., *Statistical Theory and Methodology In Science and Engineering*," John Wiley & Sons, Inc., N.Y.,

30. Anderson, T.W., *An Introduction to Multi-Variable Statistical Analysis*, John Wiley & Sons, Inc., N.Y., 1958.

31. Afifi, A.A. and Azen, S.P., *Statistical Analysis - A Computer Oriented Approach*, Academic Press, 1972.

32. Henrichon, E.G. and Fu, K.S., "Calamity Detection Using Nonparametric Statistics," *IEEE Trans. on Systems Science and Cybernetics*, Vol. SSC-S, No. 2, April 1969.

33. Kleinman, D.L. and Killingsworth, W.R., "A Predictive Pilot Model for STOL Aircraft Landing," NASA-CR-2374, March 1974.

34. Phatak, A., et al., "Analysis of Controller/System Dynamics for a Remotely Piloted Vehicle Strike Mission," AMRL (WPAFB), May 1974.

35. Bryson, A.E. and Ho, Y.C., *Applied Optimal Control*, Blaisdale, 1968.