NASA CR-163120

Advanced Flight Control System Study Final Report

J.G. McGough, K. Moses (Bendix Corp.)
J.F. Klafin (Grumman Aerospace Corp.)

BENDIX CORP.
FLIGHT SYSTEMS DIVISION
TETERBORO, NEW JERSEY
CONTRACT NAS4-2877
JANUARY 1982

NASA

National Aeronautics and
Space Administration

Dryden Flight
Research Center
Edwards, CA. 93523

NF02059

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT'D)

TABLE OF CONTENTS (CONT'D)

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (CONT'D)

LIST OF ILLUSTRATIONS (CONT'D)

LIST OF ILLUSTRATIONS (CONT'D)

LIST OF TABLES

1.0 SUMMARY/OVERVIEW

1.1 Summary

This is the final report for NASA contract NAS4-2877. This contract was to establish the feasibility, system requirements, and candidate architectures for an Advanced Flight Control System, and study potential test-beds that seem appropriate for a flight test and demonstration program. The contractor, Bendix Flight System Division, was assisted by Grumman Aerospace Corporation.

The results of the study established the feasibility of an advanced flight control system that can meet the system requirements; specifically, functional reliability and periodic maintenance requirements. Candidate architectures are discussed and a preference is justified for a distributed (parallel) microprocessor - implemented configuration. The selected configuration meets the reliability and safety criteria established by NASA and has the potential for improving software validation. Several methods for meeting the periodic maintenance requirements have been traded off; the results indicate that the number of required on-board spares is reasonable, especially in view of the trends in microprocessor reliability. Also, we have computed the efficiency of a parallel processing arrangement and it appears to offer significant advantages. A multiplexed (1553 B) bus arrangement is proposed to transmit data between servos, processors, and actuators, controlled by an ultrareliable bus controller that makes use of the NASA-developed SIFT technology. This results in an expandable, flexible system configuration.

Concerning the choice of a test-bed aircraft, it appears that the Grumman Gulfstream II, as modified for NASA's use as the Shuttle Training Aircraft (STA) offers significant advantages to NASA in terms of availability, suitability as a commercial demonstrator, and cost. Therefore, a detailed study of special airplane modification has been conducted only for the Gulfstream II.

In anticipation of the full-scale development of the Advanced Flight Control System, Bendix/Grumman are proposing, as established in section 2, several proof-of-concept and validation tasks. The accomplishment of these tasks, ahead of full-scale development rather that as part of it, will reduce program risks and establish confidence that NASA's objectives will be achieved. The tasks that we propose can be accomplished at minimum cost by utilizing NASA-owned hardware (the SIFT system and its associated test stand), facilities (e.g. Airlab), and software programs (CARE III reliability model). They comprise a validation of a SIFT-type bus controller, a reliability/safety analysis of the entire system, and a more detailed analysis of parallel processing for this application.

Grumman support during this period will address detail application of analytic redundancy and skewed sensors. In the actuation area the requirements for test programs to include electro-mechanical actuation in the test-bed aircraft will be determined. An overview evaluation of the overall system reliability will be addressed with the application of CARE III considered. A plan to provide a step by step build-up of a laboratory system to demonstrate the salient points of the FCS will be developed.

Bendix and Grumman intend to continue their association in the event that follow-on contracts, of the type described in the next section, are awarded. In the event of an award of a full-scale development and demonstration program, Grumman would be the prime contractor and Bendix a sub-contractor.

1.2 Overview of Recommended System

The Advanced Flight Control System (ADFCS) that we are proposing includes the following technologies:

- Fault-tolerant multi-processing
- Software-implemented fault tolerant computing
- Parallel processing
- Analytic redundancy
- Multi-plexed data bussing
- Direct-drive electrohydraulic control valves
- Skewed and integrated sensor subsystems
- Fiber-optic communication media
- Multi-function displays

The ADFCS is a distributed microprocessor-implemented system that is comprised of the following major elements:

- An ultra-reliable bus controller, using SIFT techniques, that is a system monitor while also controlling bus traffic and reconfiguration.

- A set of 1553B busses that carry data to and from the sensing, processing, and actuating elements of the system, EXPANDABLE, EVENTUALLY, to FIBER OPTIC LINKS.

- A set of application processors that execute control laws and other real-time computations, logic statements, and self-test programs. Each application processor will be comprised of microprocessors that perform parallel computations.

- An integrated sensor system, using a SDOF gyro configuration of hard-mounted rate gyros and accelerometers (minimum of six each) that also includes sensed data processing to the bus format.

- A set of quad-redundant actuators that process actuator command data received from the busses.

- An array of multi-function displays that receive their data, over the bus structure, from the application processors. The displays will include mode and failure annunciation status displays, and required pilot-ADFCS interactive devices.

The system is configured to include the redundancy needed to meet NASA's system reliability and periodic maintenance requirements. The precise redundancy levels which differ for the various system elements are explained in the sections below. The interconnection of the system elements is shown in Figure 30.

2.0 RECOMMENDATIONS

There appears to be no technical reason to delay a full scale development and demonstration (to commercial operators) program of the Advanced Flight Control System. The technology to make it feasible is at hand, the need surely exists in view of the near certainty that active controls will be included in the next generation of transport aircraft, and previous studies have shown that there is a highly beneficial DOC trade-off.

If, in view of budgetary or other constraints, it is not possible to launch the full-scale program, the best alternate would be to concentrate efforts on those aspects of the proposed system which (1) take the longest to verify and validate and (2) are the most risky for the overall program. Accordingly, we present in this section several tasks whose early accomplishment would greatly benefit the system and reduce program risks. These tasks are as follows: (Tasks 1 thru 5 are proposed by Bendix; tasks 6 thru 11 by Grumman).

Task 1:

We propose to utilize the SIFT hardware and its associated system test stand as a a bus controller/system monitor. Ideally, this arrangement would be validated for instance by connecting the SIFT complex via 1553B links to an array of application processors, and performing appropriate experiments on the entire system. The basis for such experiments would be the simulation of an advanced transport control system, possibly including an active control function such as is caused by relaxed static stability, as well as an autoland mode. The experiments would then include bus transfers, fault injections (single as well as multiple), reconfigurations, self-test, and environmental disturbances. The application processors could preferably be implemented in bread-board type hardware; as this may not be practical due to funding restrictions, we would propose implementing the application software on a high speed host computer in the Airlab (e.g. VAX 11/780) so that the experiments can be performed in real time. We would propose simulating in real time, application processors, and sensor and actuator interface processors, on high speed host computers resident in the Airlab facility. Figure 1 identifies the components of the simulation.

The same SIFT hardware, modified by the addition of Remote Terminals, could be used to implement application processors. In this approach, the Airlab host computers will simulate bus controllers and other subsystems.

The accomplishment of this task would increase confidence that the basic configuration can achieve the NASA requirements. This task is a basic part of the reliability and safety analyses which would, in any event, be needed for the full-scale development program.

Task 2:

Preliminary evaluation of parallel processing efficiency and overhead (see Section 6) indicates that parallel processing offers substantial benefits in performance and economy. It is proposed to conduct a more detailed evaluation of parallel processing applied to flight controls. In addition to analytical trade-offs the study would include a demonstration that a representative flight control system can be partitioned into subtasks suitable for execution in a parallel processor. This demonstration would include implementation in a prototype parallel processor in a closed-loop simulation facility. Two approaches can be taken regarding the prototype hardware:

1. Use SIFT

   The SIFT hardware configuration is ideally suited to parallel processing. This is not surprising since parallel processing is an important part of the SIFT concept.

2. Develop a prototype using microprocessors.

   The basic design would be as described in Section 6.

Task 3:

For this task we propose to emulate, at the gate-level, a dual 1553B bus controller and remote terminals and perform fault injection experiments to identify single and multiple failure combinations that result in loss of the entire bus. The emulation would include the bus interface circuitry described in Section 4.5

Task 4:

The ability to monitor the bus controller is a critical issue of the advanced architecture. It is, in fact, an important issue in any application of multiplexed data busses (e.g. 1553B). Therefore, for this task we propose to:

- develop algorithms for on-line monitoring of the bus controller;
- validate monitoring coverage, and determine the time to detect a fault and the effects of each fault before detection

This latter task would be accomplished by emulating the bus controller multiprocessor and a dual remote terminal at the gate-level and performing fault injection experiments. The effort can be reduced significantly if the multiprocessor consisted of Bendix BDX-930 processors. This emulation already exists and has been demonstrated to be ideally suited for emulating multiprocessors, such as SIFT (see Ref. 12).

Task 5:

For this task, we propose to devise a reliability model of the entire system, and to utilize NASA's CARE III reliability program as the tool for the analysis. This analysis would yield, for example, required parametric data on the effects of reconfiguration time and the effects of LRU failure rates on system functional reliability. The CARE III model can be used to optimize the configuration via a functional reliability/hardware complexity trade-off. The survivability of the system in the event of simultaneous or near simultaneous failures will also be investigated.

Task 6: Analytic Redundancy

a. Design and evaluate candidate techniques using state estimators with failure signal monitor techniques, then extend state estimator design techniques to include formulation of likelihood functions.

b. Address quantization of redundancy benefits in terms of reliability, accuracy, computation requirements, relative cost, i.e., H/W comparison monitoring vs. S/W analytic redundancy, etc., reconfiguration potential, nuisance disconnects, etc.

c. Address analytical reconfiguration techniques so that sensor and control actuators not within the local domain are used to extend the redundancy concepts.

d. Establish trades of analytic redundancy effects on system architecture.

Task 7: Skewed Sensors

a. Design and evaluate parity schemes for large numbers of sensors. The primary question is whether it is better to handle all the sensors as one system or to separate them into sub-groups. This decision requires the quantization of criteria and to address the issue of hierarchy of orthogonalization and failure monitoring.

b. Address system architecture with respect to sensor processing, data distribution, reconfiguration requirements, etc.

c. Investigate installed performance, addressing the effects of environment, physical configuration, data bus coupling, etc.

Task 8: Actuation Systems

a. Perform detailed evaluation of Direct Drive, Electro-Mechanical and Integrated Actuator Package actuation systems to determine the most appropriate candidate for the test-bed aircraft. In the case of EMA, determine the requirements for test programs in order to include EMA technology in the test-bed aircraft.

b. Address architectural considerations for the candidate technology configurations. This is to include controller type and location, self test/monitoring techniques, analog vs. digital controller trades and redundancy management techniques and requirements.

Task 9: Reliability

a. Address the problem of evaluation of overall system reliability. Investigate the application of CARE III to this problem and compare it with existing techniques.

b. Develop techniques to evaluate hardware vs. software configurations.

c. Support analytic redundancy, skewed sensor and actuation system studies.

d. Address analytic treatment of imperfect redundancy management with consideration given to being able to restore non-failed sensors which were considered to have failed between missions (they were considered hard failed in the base study). Relate imperfect failure redundancy parameters to the base sensor failure rate. Expand treatment to cover Markov analysis scenarios.

e. Perform a cost trade for allowing unscheduled maintenance vs. the baseline requirement for none.

Task 10: System Demonstration

a. Develop a plan for a step by step build-up of a laboratory system demonstration system containing the salient portions of the Advanced FCS. Initially, the laboratory system will address the avionics issues of sensor/data bus and data bus/actuator interfaces and general data bus controllers. Expansion would include sensor and actuation technology. Use of NASA AIRLAB and other NASA facilities as well as contractor facilities will be considered.

b. Develop a program for expansion of the baseline laboratory system demonstration system to a prototype evaluation system for the test-bed aircraft, leading to final configuration for the test-bed aircraft.

Task 11: Test-Bed Aircraft

a. Evaluate the impact of significant changes to be baseline system on the test-bed aircraft.

b. Update the test-bed aircraft estimate as required.

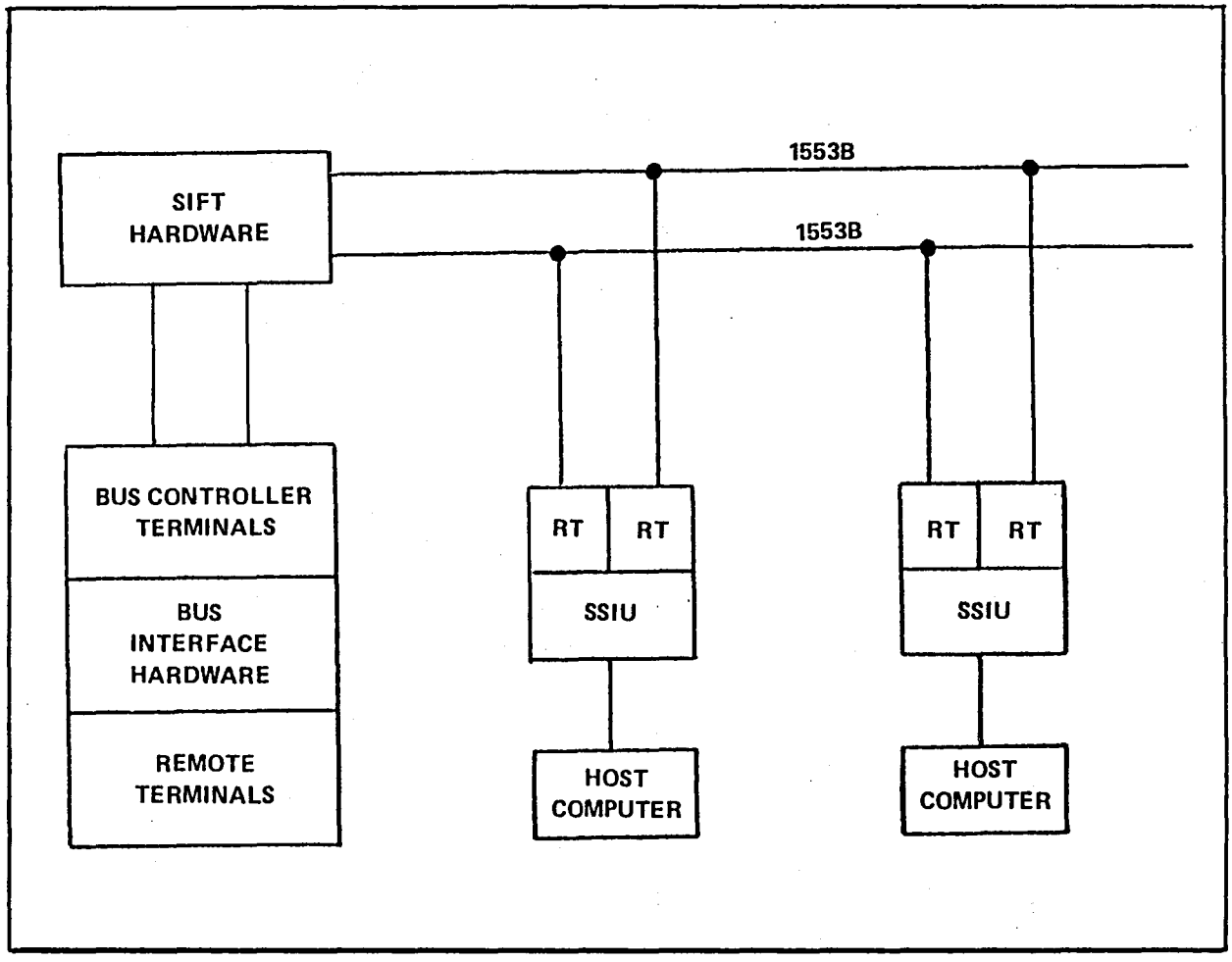


Figure 1 System Simulation

3.0 INTRODUCTION

3.1 Objectives of the Study

The principal objectives of this study as stated in NASA's SOW were to "determine, through trade studies, the feasibility and practicality of utilizing currently emerging technology to design a systems architecture that would yield an ultrareliable hybrid fly-by-wire flight control system for experiments in the near future. The system would have significantly improved performance and reliability over contemporary digital flight control systems." The system would have the following characteristics:

Active Controls	-	Ability to execute flight crucial active controls with ultra-high reliability.
Fault Tolerance	-	Ability to tolerate several faults prior to or during flight operation while continuing undegraded operation.
Dispatch	-	Ability to allow dispatch of an aircraft with failed control system elements.
Periodic Maintenance	-	Requirement for periodic maintenance only, with a high degree of integrity between maintenance periods.
Expansion Ability	-	Ability to expand the number of functions or subsystems with minimum reconfiguration of the existing system.
Technology Independence	-	Ability to accommodate hardware element retrofits without architectual redesign.

These objectives were to be realized by producing a detailed conceptual design of an advanced hybrid fly-by-wire system for a projected advanced future aircraft. This aircraft could incorporate active controls; in any event, the electrical flight control system would be flight critical for the entire flight since a mechanical back-up control system would not be included in the design. The system must be validatable on current aircraft and demonstratable to the airline and aviation communities.

The approach of the Bendix/Grumman team towards meeting these objectives was first, to recognize that an extensive technology base exists to support these objectives, and to define that technology base, and

second, to concentrate on using that technology base in formulating the basic building blocks of the Advanced Flight Control System. These building blocks include, most importantly, the microprocessor complex and the bus network. Other basic building blocks are the sensor arrays and the secondary surface actuator configuration. A system configuration that meets the above system requirements and that can be configured from building blocks that have already been validated, is the least risky approach. If such a system trades off well against other, riskier approaches, then it becomes the clearly preferred approach. However, the situation is rarely that clear-cut, and, in the actual, practical situation, some risks normally should be taken because the potential rewards are attractive. In the present case, we are recommending that the bus controller be a SIFT-type network and the microprocessor computing complex be a parallel processing complex. The SIFT concept has been mechanized and its basic applicability to the tasks envisaged here should be well accepted, while the basic concept of a parallel processing network has been well explored and validated. However, neither has been used in quite the way proposed here, nor have MIL-STD-1553-B data links been employed for the relatively high band-width requirements of flight control sensor, computer, and actuator data. So, some risks remain but they are judged to be acceptable.

On the other hand, the potential rewards of this approach are judged quite significant. They include:

- More easily validatable software
- Expandability and flexibility
- Transparency to processor architectures
- Technology independence
- Minimum configuration (cost, weight, power, etc.) to satisify the the scheduled maintenance requirements
- Minimum total software costs

A detailed description of the recommended system architecture will be found in section 5, as well as alternate systems that were considered and why they were not selected. It is emphasized that the recommended architecture builds on the successful experience with SIFT concepts, 1553B controllers, and multiple microprocessor systems.

3.2 Causes of System Failure

A detailed analysis of redundancy requirements for meeting the several system objectives has revealed that the periodic (6 month) maintenance requirement will be the driving factor that establishes how much redundancy (e.g. how many spares) need to be carried. Obviously, since this is not a direct safety-related issue, the six month term could be relaxed, in which case the conventional causes of systems failure may dictate the required redundancy. These causes are:

- Exhaustion of redundant spares due to multiple failure within mission time
- Almost simultaneous faults, i.e. a second failure during the time it takes to reconfigure from a first failure
- Latent faults not detected by a pre-flight ground test

Other causes of system failure need to be eliminated by design methodology and testing. These are, principally, design errors in either hardware or software. Such errors are sometimes called generic errors. There is no general method for eliminating such errors except for rigorous attention to detailed design methodology, careful review of all specifications (the major source of such errors), and structured software generation and validation. Alternatives such as dissimilar redundant systems or analog back-up systems are considered unattractive because they are uneconomical and raise more design problems than they solve.

Since the orientation of this program is primarily commercial, damage due to external objects (e.g. bullets) is not considered a factor in configuration design. Rather, aircraft installations should be arranged in such a manner that any localized damage (e.g. due to an engine blade separation or a localized structural failure) does not compromise the controllability of the aircraft.

Finally, the ability to correctly detect and isolate faults is a major contributor to economical system operation and to system reliability. Clearly, if the correct identification of faulty LRU's is not achieved, either or both of the following deleterious consequence may occur: Faults may stay in the system until their accumulated number overpowers correctly operating LRU's, or, more likely, resources will be exhausted prematurely as correctly operating equiment is discarded.

The system configurations that are presented in section 5 have the potential of meeting all the NASA requirements. All of the above causes of failure have been evaluated for these configurations and appropriate safety margins have been included in the design.

4.0 ASSESSMENT OF ADVANCED FLIGHT CONTROL SYSTEM TECHNOLOGIES

Fault Tolerant Multi-Processors

In accordance with Paragraph 6.1.1 of the SOW, we present here a survey and assessment of the state of the art of advanced flight control technology elements to determine their potential utility in an ultra-reliable fly-by-wire control system.

4.1 Fault Tolerant Multiprocessors

4.1.1 Requirements

For the purpose of this study, key requirements are the ability to tolerate several faults during flight operations while maintaining undegraded performance, the periodic maintenance requirements and the ability to dispatch in the presence of faults. These can only be satisfied by a system organization that can survive several similar, and many more dissimilar failures. Central to such a system is a fault-tolerant computing complex that not only must detect and survive its own internal failures, but may also be "in charge" of failure detection and reconfiguration for the entire flight control system, consisting of sensors, busses, computers, and actuators.

Further, the software for this system must be able to be validated so that confidence can be established in its integrity, and the possibility of generic (design) errors minimized. This requirements is thought to be a constraint (as well as an evaluation criterion) for the design.

4.1.2 Current State-of-the-Art of Protype/Production System

The survivability requirements for most current fly-by-wire (military) or flight-control commercial (autoland) systems are of the order of 10(-7) per hour of flight. These requirements can usually be satisfied by conventional triplex or quadruplex systems, the choice depending on whether a 100% "two fail-operate" requirement is imposed. If the "two-fail operate" requirement is not 100%, the system configuration can be triplex with self-test (e.g. AFTI-F-16); otherwise, a quad configuration is needed. It is to be noted that all current full-time digital flight control systems employ an independent back-up; this can be either a mechanical system (F-18) or an analog electrical system (AFTI-F-16). Flight-critical digital flight control systems for commercial applications are just now coming into use; so far, only non-flight critical functions have been certified (DC-9-80). However, the only flight-critical functions to be certified over the next several years are the autoland functions where the exposure time is minimal. Of course, mechanical control systems are present in all current and anticipated commercial transports.

Thus, it is clear that current useage for military and commercial digital flight control systems includes a mechanical or analog back-up system with at least level 3 (MIL-F-8785) handling characteristics. This back-up system is not needed to meet the "probability of functional loss" requirement; rather, it is included because (1) the designer, or purchaser, does not believe that the integrity of the software can be adequately demonstrated or (2) an emotional feeling that"it should be there, just in case". These two arguments are of course very similar, and, being unquantifiable are difficult to refute. The argument is sometimes clothed in terms of the need to protect against "generic software errors" (which are, in reality, design errors), but, again, this is an unquantifiable requirement. After all, design errors, unlike hardware failures, are not discovered at a constant rate. While it is possible to design a system that can survive software coding errors, this does not necessarily insure against other, possibly more prevalent design faults, such as incorrect software specifications, compiler errors etc. One method that attempts to do both makes use of "dissimilar redundancy" which is interpreted to mean that two (or more) different processors, with different software programs, are used in the system, thus virtually eliminating the probability that one common software design flaw could disable the entire system.

Aside from the additional burden that dissimilar software programs place on the entire development process, a basic objection to this approach is that the gains, if any, can't be quantified. In other words, since it is impossible to predict the probability of occurrence of a "generic software error" (or, a second or third such occurrence), detection of one such event does not yield any statistically significant information of the probability of functional survival. Nor can there be much confidence that design errors will really be detected by this method since many such errors arise from incorrect or incomplete specifications, rather than coding errors.

In Bendix' view, it is important to break with today's practice of mechanical back-up system, first, because the inclusion of such a back-up system in the design would tend to relax design discipline and possibly change design methodology; second, because it would undermine the need for the ultra-reliability and other advanced features that are the major justification for this program and last, but not least, because, if the design is credible in terms of its reliability, no back-up system is required; if not, then the proper course of action is to improve the design of the primary system to meet the requirements.

Similarly, as discussed above, we think the concept of "dissimilar processors" to circumvent the existence of design errors is a technically unsound approach which creates more difficulties than it removes.

4.1.3 Advanced Techniques for Fault-Tolerant Multiprocessors

A number of advanced fault-tolerant multiprocessor systems are currently under development for specific application to ultra-reliable flight control systems. These include:

- SIFT (Software Implemented Fault Tolerance)
- FTMP (Fault Tolerant Multiprocessor)
- Continuously Re-Configuring Multi-Processor
- Multi-Microprocessor Flight Control

SIFT AND FTMP are being developed by SRI/Bendix and CSDL/Collins, respectively, for NASA/LRC. The other two are USAF developments, the Continuously Re-Configuring Multi-Microprocessor being an in-house development at AFFDL and the Multi-Microprocessor Flight Control being developed by Honeywell under USAF/AFFDL sponsorship.

It is fair to say that (1) all of the above developments are concentrating on the computers of the flight control system, with scant attention being paid to sensors and actuators and their organization and (2) that SIFT and FTMP are further along in their development cycle than the other two systems. Further, the Continuously Re-Configuring system represents the most radical departure from current practice and hence, needs the most development. Its potential cannot really be evaluated at this time. The other three approaches suffer from the following common unresolved problems (in addition to the limitation pointed out above).

- Software validation methodology is not proven and not generally accepted.
- Bus communication networks are not designed to the ultra-reliability of the computing systems.
- A complete implementation of these systems does not exist as yet and, therefore, has not been proven.

This is not to say that some of these techniques cannot or should not be used in an Advanced Flight Control System; indeed, as described in Section 5, we propose to take elements from these approaches and combine them in our proposed architecture.

A brief description of these techniques is included for the sake of completeness.

4.1.3.1 SIFT

SIFT is a fault-tolerant computing system in which fault tolerance is achieved primarily by software mechanisms.

Application tasks are executed redundantly on multiple independent processors which are connected by a system of independently connected broadcast busses. A SIFT-type computing module consists of a processor and a memory unit. Each module communicates with every other module via a dedicated, high speed broadcast bus. When a processor writes into a designated subset of memory, the data is transmitted by an autonomous I/O controller to all modules. In this way the results of all computations are accessible by all of the processors of the SIFT computer (Figure 2). As shown in the figure, the SIFT processors communicate with the outside world via dedicated 1553 busses with each processor performing the function of bus controller for its dedicated link. A detailed discussion of how these links could be connected to other aircraft subsystems will be given subsequently. For the present discussion, the configuration of Figure 3 will suffice.

It was envisioned that the "SIFT" computer would perform all flight control, avionics and engine controls. The computations are divided, in advance, into a number of task programs in such a way that no task requires more computing power than is available from a single processor. At any given time, each processor is multiprogrammed over a certain subset of tasks. Tasks may be replicated in other processors, the level of replication depending upon the criticality of the task. Figure 4 illustrates a typical allocation of a set of tasks designated by A, B, C, D ... J, over a set of 6 processors. From the figure it can be seen that two processors may have different task allocations even though they may be executing certain tasks in common.

The control of the computing system is carried out by a number of functions that can be segmented into two classes:

1. Local Executive: performs functions that apply to each processor such as dispatching, voting, error reporting, executing new task programs.

2. Global Executive: performs functions that are global to the system such as allocating and rescheduling work load and reconfiguration.

A complete set of software functions of the Local Executive is present in each processor; those of the Global Executive are carried out in a sufficient number of processors to provide the degree of fault tolerance required. The functions are realized by programs that have the same task structure as all other programs.

The normal operating mode for a processor carrying out a task is as follows:

Data required for a task is assumed to have been computed by several processors and communicated to all processors via the internal broadcast busses. Thus, a processor commencing a task already has the redundant input data resident in its own memory. The redundant input data is voted and validated by each of the processors performing the task by comparison-monitoring. If it is arranged that the input data is identical under non-failed conditions, then any discrepancy in this data signifies a fault and is duly noted for later processing by the executive.

If the voted input is unambiguous, then the processors proceed with the task computation. The results of the computation are stored in memory and simultaneously transmitted to all other processors. When a discrepancy is detected, diagnostic programs in the global executive determine which unit is at fault. Reconfiguration is achieved by having the several versions of the global executive indicate to each local executive which tasks should be performed and which other processors should replicate the calculations for each task. All the local executives examine each of the global executive versions and independently vote on these directions. That is, each local executive decides which of the reconfiguration directions it will accept, using a majority rule. A faulty processor might not heed the directions of the global executive, but, based on the instructions of the global executive, operative processors will ignore the faulty processor.

4.1.3.2 FTMP

Another implementation of a fault tolerant system is the FTMP (Fault Tolerant Multi-Processor) system designed by C. S. Draper Laboratories.

The system architecture is essentially that of Figure 3 except that the SIFT computer is replaced of the FTMP computer.

The principal elements of this system are:

- o FTMP computer
- o Communication links between the FTMP computer and other aircraft subsystems

FTMP Computer

The FTMP computer, unlike SIFT, is a fault-tolerant computer in which fault tolerance is achieved primarily by hardware mechanisms. Application tasks are executed redundantly on multiple processors which are connected by an internal bus network as shown in Figure 5. A typical FTMP LRU is shown in Figure 6.

LRU

The LRU consists of:

- CPU processor and code memory
- Shared memory
- I/O module
- Bus Guardian Unit
- Bus Interface Unit
- Clock
- Power Supply

Tasks are allocated to redundant CPU's which operate in triplicate in tight (i.e., in bit) synchronism. The triad members perform identical operations, on identical data, forming identical results. Three copies of all data are sent simultaneously on three independent serial busses (e.g., A, B, ... E of Figure 7), one from each member of the triad. Errors are detected and masked at the receiving device by the Bus Guardian Unit, which uses a majority vote on each transmitted bit.

To reduce bus loading each bus consists of four lines each of which is dedicated to a specific task: 1) Clock bus (G), 2) poll bus (P), 3) transmit bus (T), 4) Receive bus (R), as shown in Figure 7.

When a fault is detected the faulty unit is identified and replaced by a spare unit. If no spares are available the triad is disassembled and its non-faulted units become spares for the rest of the system. When a fault is detected the BGU's inhibit the faulty processors' access to the busses, thus, effectively disengaging the processor from the system.

Data between other aircraft subsystems and FTMP is controlled by the I/O module which acts as 1553 bus controller and as I/O port for access with FTMP. These modules are not configured in triads in FTMP because aircraft sensors and actuators are not triply redundant on the external bus. Data redundancy is established after reception by the processor using "interactive consistency" techniques (D). (Ref. 1)

The redundancy used in FTMP requires tight synchronization of the executed tasks and the transmission and reception of bus data in order to facilitate the hardware voting of the Bus Guardian Units. The timing reference is obtained by employing a redundant clock system. This system utilizes four independent phase-locked crystal oscillators connected in a majority logic inter-connection scheme (Ref. 2).

The shared memory contains the resources necessary to reallocate tasks within the FTMP complex. These units contain stored programs and intermediate data from task computations, such as integrations. The shared memories also act in triads in the same way as the CPU's and cache memories.

In many respects FTMP operates like SIFT, e.g., tasks are allocated to individual processors which operate in redundant sets. Tasks are reallocated when faults occur, depending upon available system resources. Both systems are distributed since tasks are executed by independent processors. The main differences are:

1. Failure detection in FTMP is achieved through hardware mechanisms, whereas SIFT utilizes software.

2. SIFT imposes but few constraints on its constituent processors and busses whereas FTMP requires very specialized hardware.

4.1.3.3 Continuously Reconfiguring Multi-Microprocessor (CRM2FCS)

The following summary description of this intriguing system is based on reports published by USAF/AFWAL (Ref. 3).

The CRM2FCS design centers around a system of autonomous microprocessors connected by a common set of serial multiplex busses. These processors operate in a pooled configuration where any processor can perform any task at any time. Further, task assignments are continuously redistributed among all processors in a never-ending process of reconfiguration. If a processor fails, it is left out of the next reconfiguration cycle and the system continues to operate without any adverse effect. There is no central controller in this system.

A diagram of the architecture is shown in Figure 8. The SIM (State Information Matrix) is a mathematical abstraction used for organizing all the available information about the state and environment of an aircraft. With this structure all microprocessor functions can be broken down into three sets. The first set of functions takes raw sensor data, processes, filters, and stores it in designated locations within the SIM. Another set of functions takes information which is in the SIM, processes it, and refines it to produce higher quality data. This could be, for example, a Kalman Filter algorithm. This refined data is stored back in the SIM where it can be accessed by other processors in the system. A third set of processor functions take information from the SIM and processes it for use by the outside world. These are typically control laws or display algorithms. With the SIM structure, all software programming for each microprocessor has been reduced to a single set of interactions with the state information matrix.

The implementation of the virtual common memory in hardware (shown in Figure 8) utilizes a simple serial bus structure. Each unit interfaced to the serial bus is referred to as a processing module. A processing module consists of a microprocessor, local memory, transmitter, receiver, and a copy of the state information matrix. Each processing module independently determines which task it must do next. It accesses variables from the local SIM which are needed to do a computation. When the algorithm has been completed, the data and its location in the SIM are placed in the processing module's transmitter buffer. The transmitter circuit automatically searches for an available bus and transmits the information. Every processing module receiver, including the originating processing module, receives the data. Through a direct memory access, the data is then placed in the proper location in the SIM of every processing module. Each processing module maintains an identical copy of the SIM. As far as any processing module is concerned, the SIM appears to be entirely within its own local memory. Using this concept, processors connected by a simple serial bus appear to share one common memory containing all information in the system. This greatly simplifies programming by reducing interprocessor communication to simple reads and writes on a virtual common memory.

In the figure, six processing modules are shown connected to a set of four common data busses. Each data bus consists of one clock and one data line. Information is transferred between processors using a simple serial multiplexing scheme. Processors compete for access to the busses. In the event that two transmissions "collide" only one message survives while the other one is automatically re-transmitted as soon as the bus is free. Thus, one of the advantages of this scheme is that it uses busses efficiently. Another advantage is that latent failures are not likely to remain latent for very long. Also, failure transients due to reconfiguration are minimized (as they are in SIFT, FTMP, etc.).

An example of what is meant by continuous reconfiguration is shown in Figure 9. A system of 9 processors is shown performing 6 different tasks, A thru F during three consecutive time frames. During the first time frame processor 1 is doing task B, processor 2 task D, processor 3 is a spare, and so on. In continuous reconfiguration the tasks are redistributed among the processors at the beginning of every time frame. For example, in the second time frame, there is an entirely different assignment of tasks to the processors. This reassignment is accomplished by having all of the processors that are currently healthy in the system compete for task assignments. If a processor fails during any time frame, it is no longer able to compete for task assignments. If processor 4 failed during the second time frame, then during the next frame, it would not be able to compete for task assignment. The 6 tasks which need to be done are taken by healthy processors and the 2 remaining processors become spares. In other words, a failed processor simply disappears from the system without any other processors being aware that it is gone.

There are a number of advantages to the continuous reconfiguration approach. One of these is the ability to have continuous spare check-out. In traditional systems, where certain processors are permanently assigned to the spare status until they are needed, it is possible for one of these processors to fail while functioning as a spare. When a system processor fails and the failed spare is brought on line, catastophic results may occur. The technique of continuously switching which processors are acting as spares allows every processor in the system to be constantly exercised.

Latent fault protection is another advantage of the continuous reconfiguration approach. Latent faults are a class of faults that are characterized by the partial failure of a processor. The processor failure is not immediately detectable and may impede the systems ability to recover from any subsequent failures. Continuously exercising each processor, so that over a period of time every processor performs every task, forces a partially failed processor to reveal its failure and be removed from the system before it can interact with another partially failed processor in a manner that may preclude recovery.

A third benefit of continuous reconfiguration is zero reconfiguration delay. Most systems that are reconfigurable treat a failure as an emergency requiring special processing. This produces delays and possible failure transients in bringing the system back to its fully operational state. With continuous reconfiguration there is no emergency. The system reconfigures naturally every time frame so that, when a failure occurs, the system takes it in stride and with no failure transient.

It is claimed, by the CRM2FCS investigators, that the benefits of this approach include the ability to reduce software costs, the possibility of greatly reducing unscheduled maintenances (by adding many more processors than are necessary to prevent loss of function), and the ability to expand the system, including software additions without re-programming. No evidence exists at this time that these claimed benefits can, in fact, be realized. Also, there are a number of basic questions that need to be answered before a realistic assessment of this system can be made. Among them are: (1) How are failures detected and (2) What mechanism keeps track of failures? Bus loading and contention delays may also impose constraints on system performance.

At this time, this approach is not a viable candidate for an Advanced Flight Control System implementation phase. However, further development of this concept over the next year or two could cause us to revise our opinion.

4.1.3.4 Other Multi-Processor Configurations

Using microprocessors as basic building blocks, it is possible to devise parallel processing arrangements that divide the computational load in a logical, pre-arranged manner. An example of such a parallel processing arrangement is discussed later on (Section 6). Another, similar parallel configuration is being developed for USAF/AFWAL by Honeywell under the name of Multi-Microprocessor Flight Control. These arrangements are not, by themselves, ultra-reliable, fault-tolerant multi-processors (in the sense that SIFT and FTMP are); rather their basic objective is to achieve higher thruput without surrendering the simplicity, low cost, and potential software simplifications obtainable through the use of microprocessors. It is of course possible to construct a SIFT-type multi-microprocessor system that is in all respects equivalent to the current miniprocessor-based SIFT System, and, as detailed in Sections 5 and 6, that is the approach we intend to pursue. This arrangement will result in a more structured software program and one that is more maintainable.

Specifically, we want to arrange the software so that, in the event of a change, only that section of the software affected by the change needs to be revalidated. We believe that this goal, which should result in lower software costs, can be achieved with a parallel processor/SIFT arrangement.

Such an arrangement has the further advantage that it is more easily expandable than architectures that inherently depend on multiples of microprocessors. For example, not all functions of a Flight Control System are flight critical (especially in the case of commercial transports) and of

course, non-flight critical functions do not require the redundancy of flight critical functions. In a parallel processor/SIFT architecture, we can accommodate such a requirement with a single (non-redundant) processor; in a multiple microprocessor arrangement, a multiple processor (minimum of two) must be added. There appears to be no reason to pay this penalty.

Finally, it is desirable to implement the redundancy management and bus controller algorithms in separate hardware so that applications software changes (which occur relatively frequently) do not require re-validation of redundancy management software. As pointed out above, the application software is further structured so that changes that affect only one axis of control, for example, only require that the software for one of the parallel microprocessors must be re-validated.

4.1.3.5 Concluding Remarks

While microprocessor technology may be expected to achieve further improvements in speed (thruput), size, weight, and reliability, this will not, in our view, lead to system concepts that are radically different from those outlined in the previous sections. The basic parameters of an appropriate architecture for an Advance Flight Control System involve the redundancy management, the organization of the application processors (parallel or not), and the bus controller and network organization, and these parameters can realistically only be chosen in the manner discussed above (including, or course, the possible variations that have been described) if the system requirements are to be met. It is difficult to think of suitable configurations that differ in essentials from those described herein.

The risks of our approach are minimal because the proposed system architecture is a direct extension of SIFT/FTMP concepts. These concepts have been thoroughly studied and proven by simulation and emulation techniques. Breadboard hardware has been built in both cases and is currently being evaluated. Design changes have been identified and incorporated into the hardware. The interface with the 1553 bus has been validated.

The remaining issues are: (1) the use of the redundant 1553B bus in a fail-operational configuration and (2) the validity of the ultra-reliable bus controller concept. Obviously, a detailed system failure modes and effects analysis needs to be conducted to ensure that there are no common failure modes in the design and that all failures are, in fact, detected. Specifically, a SIFT/FTMP type of computer complex has not heretofore been connected to an aggregate of redundant sensor and actuator subsystems via a

set of multiplexed busses and the possibility of bus failures disabling or defeating, in whole or in part, the redundancy management algorithm must be investigated, using the FMEA or a system emulation (on an appropriate host computer). However, as is shown in subsequent sections, we do not think doing so presents any inherent difficulties, but that the design concept is sound, and that the communications problem is solvable.

4.2 Software Implemented Fault Tolerant Computing

4.2.1 Software/Hardware Trade-Offs

The SIFT approach offers economies in hardware, which on a recurrent basis, appear quite attractive even though the relative cost of hardware is now less than it was when this philosophy was conceived. It suffers from two disadvantages; first, that it put an extra computational burden on the processor (redundancy management algorithm and peripherals can take up to 35-45% of the total required thruput) and it increases the software task, i.e., the amount of software that must be generated and validated. As to the first, any thruput limitation on the processor is alleviated by the parallel processing approach, and of course, processor thruput capabilities are increasing. With 4 processors in a parallel complex, for example, even systems that conventionally are "squeezed" for thruput, will be able to "coast", since the overhead is low (see Section 5.7). As for the software, to be sure, there is somewhat more of it, but, again, the system architecture permits a decomposition of the total software into small modules whose generation and validation is more easily managed. So, while there is, overall, a greater amount of software, it is more easily structured using the distributed approach and therefore more easily validated and verified. We do not think that this is an unfavorable trade-off.

Experience with Digital Flight Control Systems (e.g. AFTI F-16) indicates that typical real time utilization is approximately as follows:

Redundancy management/monitoring	43%
Control laws processing	32%
Overhead (Executive, MUX interface, I/O processing)	25%

The AFTI-F-16 approach is like SIFT in that all the monitoring and voting is performed in software. The above percentage of real time that is taken up for redundancy management and monitoring is, therefore, the maximum; to the extent that some output monitoring is performed in the

actuator packages, this percentage will decrease. It is very clear that a software-oriented approach is feasible even with today's technology, is probably the most economical in the long run, and is really constrained only by the well-publicized difficulties of software validation.

4.2.2 Software Validation

We have reviewed many schemes for implementing and validating software that purport to be an improvement over the standard validation method, i.e. test and test and test. Among these methods are:

- Dissimilar redundancy in programming (N-version programming)
- Dissimilar redundancy in hardware and software
- Recovery block technique
- Proof-of-correctness of software
- Combination approach

We discuss each of these in turn but it can be said, at the outset, that they all tend to complicate the design and the validation processes, for what seems at best to be marginal gains.

In putting the "software problem" in perspective, it may help to identify the principal causes of software "failures". Obviously, all software "failures" are really specification, design, or coding errors. The latter are, in our experience, detected fairly readily during the various software tests (e.g. module tests, system tests) that will be employed. It is the errors resulting from faulty or incomplete specifications (the principal cause of software "failures") that are the most worrisome because they are the hardest to detect. Thus, the above techniques can most logically be evaluated in terms of their ability to detect these "failures".

It is of course clear that one must start with a basic system specification that is correct. No validation scheme could detect errors in that basic document. However, the next level of detail, typically represented by a Computer Software Requirements Document (CSRD) and then a Computer Software Design Document (CSDD), is where misinterpretations, omissions, inconsistencies, etc. can cause errors that will, eventually, be reflected in incorrect or incomplete code. The coding itself, assumed to be done via an HOL and a validated compiler, can of course produce additional errors.

If dissimilar redundancy, in either hardware or software, is employed, the number of specifications is increased and so is the probability that errors are committed in writing them. This would be no cause for alarm if there were a greater assurance of success, by virtue of the dissimilar implementation, of detecting these errors. However, this would only be the case if the two CSRD's or the two CSDD's were sufficiently different, i.e. included different interpretations of the basic system document. While one can obviously make up scenarios where the dissimilar software (or hardware) would yield a benefit, one can make up other, equally plausible scenarios where it would not. In short, this approach would doubtless detect some coding errors, but very few software design errors. Considering that the software design and validation task is now at least doubled, that seems a high price to pay for such a small benefit.

In the method of Recovery Blocks (due to Randall (Ref. 4)) an acceptance test is employed to ensure that the output of each software task yields an "acceptable" result, and a watchdog timer ensures that this output is available in a timely manner. If this does not occur, an alternative software "path" is activated to compute the same task. (The watchdog timer can be used independently of Recovery Blocks and is so used in all Bendix software). The key to the Recovery Blocks is the development of an acceptance test that will catch software failures in time. Such a test would be, in general, quite difficult to devise. However, if it could be devised, then, equally likely, the error which it is supposed to detect must be known, and then there is no need for the test in the first place. Thus, it seems to us that the use of this technique to detect software errors is not appropriate since it does not promise to solve the real software design problems. The test would seem to be more appropriate to hardware error detection.

The "Proof-of-Correctness" (Ref. 5) method for validating software is being investigated by SRI, Inc. as part of the SIFT Program. The basic idea seems to be to so structure the software so that it can be regarded as a (nested) series of assertions that can be rigorously proved via the techniques of mathematical logic (predicate calculus). It appears, however, that this method "works", if it does at all, only for those parts of a flight control problem that can be represented as logic statements, surely not the total flight control program. Also, the technique is not readily understandable to the engineering community and therefore probably not acceptable. As of this date, its usefulness has not been demonstrated.

In addition to a rigorously structured approach to software generation, and exhaustive testing at several levels, it is cost-effective to include software reasonableness tests, i.e. tests that can detect when a

variable has assumed unreasonable values, when a surface is commanded to a hardover position, etc. Clearly such tests have a limited application, but they are useful and don't cost much (in real time, memory etc.). Since their effectiveness is considerably less than 100%, no credit is taken, in the reliability calculations, for the failures detected (hardware or software) by these tests.

4.2.3 SELF TEST

An in-flight background self-test can detect hardware failures with an overall coverage of 95%-98%, i.e. that is the percentage of all failures that will be detected. The Advanced Flight Control System should include an in-flight self-test for the following reasons:

- It is an alternate to the comparison monitoring method of failure detection, which in fact can readily isolate the failed channel, or LRU, and can confirm the failure once the faulty channel is removed from on-line operations.

- The in-flight self-test may be considered a part of the maintenance and pre-flight self-tests, thus, they must be implemented anyhow and the required memory must be provided. If an in-flight real-time squeeze develops, the self-test can be run on alternate cycles, etc.; thus the real time usage can be made minimal.

- No credit is taken, in the reliability calculations, for the potential contribution of self-test to the system's probability of survival. Because of this conservative ground-rule, it will not be necessary to prove the percentage of coverage. Self-test results will not be permitted to throw "good" LRU's off-line unless comparison monitoring failure logic has already indicated a failure.

- Self-test exercises parts of the program (e.g. flare) that may otherwise incur latent failures. An accumulation of latent failures could defeat the failure detection algorithms.

4.2.4 Failure Detection

The principal method of failure detection is comparison monitoring. LRU's, that is, sensor processors, application processors, bus controllers, actuator processors, etc. will be voted in triads or "by fives", to mask the effect of any failure. Spares, when available, will be substituted for failed units.

Comparison monitoring is the best failure detection method with respect to coverage, i.e. all failures above the comparator threshold are detected. Speed of failure detection can be suited to the system design requirements; this parameter must be traded against nuisance alarms and the probability of premature exhaustion of available resources. Persistence counters and sophisticated algorithms such as sequential probability ratio tests are employed to minimize the false alarm rate.

Failure detection can be implemented in software or in dedicated hardware. We are proposing that most of the fault detection and identification algorithms be implemented in software, because this results in a system with less weight, greater reliability, greater flexibility to changes, and lower cost relative to hardware-implemented algorithms. The principal disadvantage of this approach has always been the relatively long execution time that these algorithms require.

We believe that the use of a SIFT-like ultra-reliable bus controller make it reasonable to incorporate the failure detection software in that controller. The SIFT organization and software structure is peculiarly well adapted to logic statements (rather than number-crunching as in control law implementation). This of course also reduces the thruput requirements of the individual microprocessors so that standard, economical units can be selected.

4.3 Analytic Redundancy Overview

4.3.1 Introduction

The advent of full authority digital flight control systems and their associated reliability requirements has given prominence to the areas of fault detection, redundancy management, analytic redundancy, failure tolerance, etc. Any fruitful discussion of these areas must start by applying accepted definitions to these terms and describing their relationships. A review of engineering application will then be presented along with suggestions as to the path future work should follow.

A Redundancy Management (RM) system is that part of the flight control system which manages the sensor, and possibly actuator, complements in such a way as to insure the required n fail-op performance. Included under this umbrella called "redundancy management" are items such as fault detection and isolation (FDI) which refers to the process by which a failed or erroneous complement is identified and isolated from the correctly operating portion of the Flight Control system. The fault detection process may be a simple pass/fail test (i.e. gyro spin motor sensors) or

may be a very sophisticated statistical test on the "goodness" of the sensor output, (i.e., signal error whiteness). Once the fault is detected the next step is to remove the offending component off-line either momentarily in the case of a transient failure, or permanently for a permanent failure.

Analytic Redundancy (AR) is a term which is defined as the use of known physical relationships in the performance of a Redundancy Management System. It has been described as a "general failure detection process", (ref. 19). Specifically, the known physical relationships are utilized to derive expected measurements, likelihood functions, parity results, etc. to determine if a sensor is failed and more specifically which sensor has the highest probability of being the failed component. Once the component has been identified the Redundancy Management System will take the appropriate isolation action.

A survey of current work in this area gives good evidence of the validity of the analytic redundancy concept along with some of the problems. The major conclusion which can be drawn from the work summarized in Table 2 is that Analytic Redundancy can give good performance in terms of failure detection provided that adequate knowledge of the sensor characteristics during a failure is available and is correctly modeled when designing the system.

Analytic Redundancy (AR) may be applied to all the components of a Digital Flight Control System (DFCS). The derived relationships are not only used in detecting failures, but are used to either "replace" the failed sensor through a derived signal or reconfigure the DFCS to maintain flight performance, allowing for the possibility of failed control surfaces, (refs. 20, 21). Through the use of AR highly fault tolerant DFCS designs are possible.

There are several techniques which can be utilized to perform the Analytic Redundancy function. A brief summary of some of these and their possible applications are presented in Table 3. Obviously some of these techniques would be extremely difficult to implement due either to software/hardware requirements (multiple hypothesis testing or parameter identification) or to the fact that these techniques are not yet out of the research phase (i.e. jump process analysis).

4.3.2 Proposed Analytic Redundancy Schemes

Using the accepted definition of analytic redundancy as a "general failure detection process", a series of methods will be presented along with associated advantages and disadvantages.

The simplest method is comparison monitoring of like sensor signals. The obvious advantage is the fact that no complicated software (or hardware) is necessary to implement the scheme. Disadvantages include high false alarm rates, difficulty of comparing skewed or unlike sensors, and the possible requirement for a large number of sensors to meet operational specifications.

By accepting incremental costs in software and memory requirements, redundancy management can be performed through the use of parity equations. Based on a sensor complement's geometry, it is possible to form linear combinations of subsets of sensors which will equal zero if no errors (or failures) are present. Non-zero parity values are caused by the presence of errors in sensor data. Through the use of simple corrections for lever arm and structural effects, parity methods can give good P(detection) of failures as well as low false alarm or nuisance alarm rates. This technique has proven very effective when utilized in skewed sensor systems, (refs. 20, 21).

If the P(detect) requirement is very high, the next step is to use a form of diagnostic filter along with generalized likelihood methods. This requires one or more state estimators along with the associated software and possibly a higher speed (and larger memory) CPU. These methods are extremely flexible in that they allow the use of unorthodox sensor geometry and multiple combinations of dissimilar sensors. Also, using these more complex schemes may give lower nuisance alarm rates. The major disadvantage of generalized likelihood or hypothesis testing methods is the need for a priori knowledge of sensor failure signatures (i.e., how the signal changes with particular modeled failures). This will require a more detailed knowledge and model of the particular sensors for an effective design.

4.3.3 Proposed Generalized Likelihood Implementation

The Generalized Likelihood approach assumes that postulated failures give recognizable signatures which are known a priori. Therefore a set of hypotheses can be stipulated i.e.,

h_o = no failures

h_i = bias failure sensor 1

h_m = soft failure sensor 1

h_z = unmodeled or unknown failure or transient failure.

In order to determine the correctness of any hypothesis, the necessary information can be obtained through the use of a State estimator which takes in raw sensor data and develops estimates of modeled states based on this raw data and knowledge of certain stochastic properties of the measurements. Based on the estimated states in Figure 10, expected values of the measurements, $y_k(\hat{y}_k)$, can be formed. By including in the estimated state vector such quantities as sensor bias states, etc. sensor failures may show up as sudden changes in the values of the residuals $(y_k - \hat{y}_k) = \epsilon_k$. If the residuals, $_k$, are used to generate likelihood functions $L = f(\epsilon_k, Pm)$ (Pm is the associated covariance matrix) the correct hypothesis (h_i) can be determined by the value of L. If the indeterminate hypothesis, h_z, is indicated by more than, say 2-3 samples, then a backup detection scheme such as comparison monitoring or parity equations may have to be used to identify the particular failed sensor. Figure 10 is a simplified block diagram of this proposed scheme.

Some of the points which must be resolved in the course of a design effort include detection of soft failures (i.e., null, or scale factor shifts), how many different failures must be hypothesized, computational loads due to matrix manipulations, etc.

For detection of soft failures, if a skewed configuration is assumed, the problem can be solved by a simple comparison between estimated or expected and actual sensor outputs since the sensor is receiving inputs from more than one axis. This type of failure should lead the appropriate element of ϵ_k to be large enough to noticeably change the value of L leading to an indication of a failure hypothesis, h_i.

For bias type failures (hard over, etc.) comparison of the estimated vs. actual sensor data can also be used as well as the resulting likelihood function value. Alternate tests could be zero-mean tests on ϵ_k, the residual, and ramp-like changes in values of L etc.

The required number of failure hypotheses will have to be determined based on the sensor number and configuration. A possible first assumption is that each sensor have 4 modes h_1 = all ok, h_2 = bias failure, h_3 = soft failure, h_4 = indeterminate status.

Computational loads can be determined by considering the number of states and measurements in the estimator as well as the matrix operation required for generating $L = f(\epsilon_k, Pm)$. Based on the number of operations for these two functions, and the number of operations to perform other functions such as Fault Isolation, Built in Test, etc., a computer throughput requirement can be determined.

One area of interest in the generalized likelihood scheme is that of formulating the residuals in such a way as to magnify the failure signatures thus making them easier to detect. This area should be investigated in the early stages of any design effort.

Other areas of interest are: determination of p(detect) for depleted sensor sets, p(detect) for multiple simultaneous failures and threshold (magnitude and time) values for determining h_i.

The final part of the design effort should be a laboratory verification of as complete a system as possible so as to insure the viability of the generalized likelihood method.

In order to determine the advantages of using the more complex generalized likelihood method for AR, it is suggested that the backup FDI scheme be one which has a proven fault detection ability to do the FDI task, specifically a parity-space scheme may be used. In this way the new scheme can be tested against a known benchmark.

In summary it is suggested that a study be undertaken to determine the quantitative benefits of doing Analytic Redundancy utilizing the Generalized Likelihood Method for Fault Detection and Isolation. This work will define such criteria as software costs, hardware requirements, nuisance alarm rates, probability of detection P(detect), probability of multiple failure detection, effective system performance in presence of multiple failures, etc. Another area which will be investigated is that of the adequacy of sensor models and associated knowledge of failure characteristics which is needed to insure good performance of any likelihood type of detection method. Table 4 is a summary of some specific design goals and the recommended methods to achieve these goals.

4.4 Actuation System Technology

4.4.1 Introduction

Various aspects of actuation system technology are being studied by the Navy, the air Air Force and NASA. Current prorams are directed at investigations of:

- electromechanical actuation systems
- Direct drive valves
- Integrated actuator packages

- Light weight/high pressure hydraulic systems (8000 psi)
- Rotary actuators, both electromechanical and electrohydraulic

All current actuation systems programs were reviewed for potential application to the Advanced Flight Control System and a brief description of each program is included in this survey. Table 4.4-1 contains a summary of the characteristics of the different approaches and a statement of the developmental status of the program.

Table 5 also presents a forecast of the availability of the technology in terms of committment to the design of a planned aircraft and expected schedules for currently planned R&D flight test programs.

4.4.2 Electromechanical Actuation Systems (EMAS)

An electromechanical actuation system consists of three basic elements:

- An electric motor(s) driven gear box/actuator assembly that controls and powers the aerodynamic control surface or thrust vectoring device
- Solid state, high power switching devices that provide power to the actuator
- A microprocessor controller that provides:
  - electronic computation
  - high performance capability
  - variable and controllable motor characteristics such as:

    torque; RPM; frequency; rate; commutation characteristics
  - position and dynamic feedbacks available as control elements

EMAS can be configured as linear or rotary actuation systems and in either velocity or torque summer configurations. Various redundancy levels may be accommodated in the designs, although, as is also true in dual tandem hydraulic actuators, the redundancy level is generally reduced to dual in the last stage and the final connection to the control surface is a single structural load path.

The major EMAS programs that have been recently completed or are now underway are:

- Boeing Military Airplane Co. Study - AFWAL funded "Airplane Acuator Trade Study".
- Rockwell International Study - AFWAL funded "Airplane Actuator Trade Study:
- Honeywell/Inland Motors Program to develop an EMAS for the Space Shuttle Elevon
- NASA/Johnson Spacecraft Center EMAS Development Program for the Space Shuttle Elevon
- Lockheed California Co. Studies of "All Electric" Transport Aircraft
- Boeing Commerical Airplane Co. Studies of "All Electric" Transport Aircraft and EMAS Development, Test and Flight Test Programs
- Grumman Aerospace Corporation. EMAS Studies, Development and Test Programs - Funded by Naval Air Development Center.

The two AFWAL funded "Airplane Actuation Trade Study" programs are scheduled for completion in late 1981 or early 1982. The baseline aircraft are Air Force advanced fighter concepts. The studies are comparing advanced hydraulically powered actuation systems with electromechanical actuation systems and with Integrated Actuator Packages (IAP).

The Honeywell/Inland Motors program is jointly funded by the two contractors and NASA/JSC. The program is directed toward development of an EMAS for the Shuttle inboard elevon. Prototype hardware has been manufactured and is currently being tested at Honeywell's Clearwater, Florida facility. The actuator is a direct replacement for the hydraulic actuator now used to drive the elevons on the shuttle. It fits within the space envelope, meets the performance requirements, utilizes the same structural mounting and drive interfaces and uses significantly less power.

The Lockheed California Co. study was funded by NASA/JSC and the final report was published in July 1980. The study evaluated EMAS for 3 classes of commercial transports:

- An Advanced Transport Airplane (ATA), a 500 passenger advanced version of theL-1011 airplane
- A short haul 50 passenger airplane
- A short haul 30 passenger airplane.

The study showed significant savings in energy, fuel, life cycle costs and weight based on the combination of EMAS and the elimination of engine bleed air. In all, 29 flight control actuator configurations were studied and 3 types were designed.

The Boeing Commercial Airplane Co. program is directed at 100 to 500 passenger "all-electric"transport aircraft. Key developments are an all electronic cockpit, EMAS for primary flight controls, elimination of engine bleed air, digital FBW and extensive use of a digital data bus system and voice acquisition to computers and voice synthesizing for alert and warning messages. Current plans include a flight test program with EMAS driving roll control surfaces in the wing and later one of the two rudder surfaces on a 727 aircraft.

The Grumman study is currently funded by NADC and in prior phases has evaluated:

- An EMAS to power and control the canard control surfaces on the Grumman Design 623-1024, a Navy Type B V/STOL supersonic fighter airplane.
- A modified AFWAL/AiResearch EMAS to power and control one of the two rudders on an F-14, in a flight test demonstration program.

To date, the program has shown that the EMAS approach is feasible for a high performance fighter/attack airplane and that an EMAS can be designed for the critical application (canard) without resorting to active cooling or energy storage techniques and that all performance requirements can be satisfied. The F-14 flight test program is planned for late 1984 or early 1985.

The AFWAL funded AiResearch program was conceived in 1972 and culminated in development of a dual motor, velocity summed EMAS using 270 VDC samarium-cobalt, inside out, brushless motors. The EMAS includes the actuator, solid state switching/inverter assembly and a controller. Features include: electronic commutation; current limiting; rotor position, current, rate, motor and actuator position feedbacks. The unit weighs 35 lbs and has undergone environmental and performance testing. Specific performance data is:

- No load rate - 95 deg/sec
- Stall load - 70,400 in-lb
- Bandwidth - 13 Hz @ $\pm$ 1 deg
- Peak output power - 8 HP

The general conclusions of all the programs to date were summarized at a NASA workshop in Hampton, VA in June 1981. The general conclusions were:

- Lockheed & Boeing have proven feasibility and benefits for 30 to 500 passenger airliners
- Honeywell and Johnson Spacecraft have proven feasibility, benefits, and design for Space Shuttle
- Grumman has shown feasibility for Supersonic Fighter/Attack Aircraft
- Numerous systems/hardware suppliers have the know-how, expertise, and developed technology to proceed

But Proceeding Means

- Refinement and, in some cases, development of hardware to unique flight control, system requirements
- Demonstrating reliability of gear boxes and power switching /inverter modules
- Developing fault tolerance, reliability, redundancy, and redundancy management philosophies
- Developing electrical power supply requirements, configurations, laboratory, and simulation test systems as well as systems for flight test evaluation.

The general consensus of opinion was that an "All Electric" demonstrator aircraft should be developed and flight tested and that one or more limited flight test programs should be completed as a build up to the "All Electric" demonstrator. No one expected that a committment to incorporation of EMAS into a production aircraft design could be made prior to 1990.

4.4.3 Direct Drive Valves

A direct drive valve has been defined as a conversion and amplification device in which an electronically signalled motor directly positions a main control valve. Figure 11 shows the typical 2 stage EHV mechanization, the direct drive valve mechanization and a compromise "staged" direct drive valve.

Benefits of the direct drive valve concept are:

- Reduced servo actuator complexity/cost eliminates hydromechanical failure monitors
- Reduced electric wire count
- Reduced maintenance
- Hydraulic systems savings
  - Eliminates EHV null flow losses
  - Reduced heat exchanger requirements
- Substantial weight savings
- Simplified interface of multiple signal channels with 2 hydraulic systems

Problem areas or potential concerns are:

- Increased electrical power level
- Electromagnetic interference of power switching electronics
- Reliability base for jam-free motor and valve combination
- Chip shear forces tend to be low

There are several direct valve programs underway. Some are company funded efforts and others are funded by AFWAL or NADC. Figure 12 presents a summary of some of the programs recently completed or now underway.

4.4.4 Integrated Actuator Packages (IAP)

IAP's have been defined as an electrically powered and (usually) electrically controlled package ocnsisting of an electric motor driven hydraulic pump which provides power to a hydraulic actuator; hydraulic circuit is complete including filters, reservoir, heat exchanger, etc. Control is usually provided by a servo valve which either modulates the pump yoke and, therefore, actuator flow (servo-pump IAP), or modulates the actuator by means of a servo valve supplied by a pressure compensated pump (servo valve IAP).

Figure 13 presents a simple comparison of the conventional central hydraulic system(s) approach with the IAP approach.

Boeing Military Aircraft Co., Sperry Vickers, Bendix Electrodynamics and North American Rockwell are evaluating IAP's, for use in military or commercial transport aircraft. Boeing plans to convert the YC-14 to an all EMAS aircraft. There are several different types of IAP's under consideration and in evaluation in the current programs. Results of the current programs should establish the feasibility of the concept and the advisability of incorporating IAP's into new aircraft.

4.4.5 Light Weight (High Pressure) Hydraulic Systems

NAVAIR and NADC have funded studies underway that involve North American Columbus Division of Rockwell International, Vought, Grumman and several equipment suppliers. The program objectives are:

- Develop an 8000 psi hydraulic system
- Provide substantial weight and space savings
- Improve Maintainability and Reliability.

The program goals and benefits are achieved by:

- Specification changes
- Specific vehicle design ground rule changes
- Changing design pressure from 3000 psi to 8000 psi.

A general summary of the findings to date are:

- Weight savings of 27-30% possible with changes to current military specification requirements
- Changing design margins/ground rules will make hydraulic systems lighter without impacting reliability
- Light aircraft appear to have approximately the same percentage weight savings as larger aircraft
- Testing of tubing, fittings, actuator, valves, and seals have been satisfactory todate and no obvious technical problems have surfaced
- Most aircraft in the design phase go for all possible weight savings due to program incentive
- Airlines pursuing 100 and 200 lb weight savings to improve fuel consumption statistics.

The present phase of the NAVAIR/NADC program will culminate in an 8000 psi flight test program in an A-7 aircraft. Laboratory testing is continuing at Rockwell, Vought and Grumman.

4.4.6 General Discussion

Electromechanical actuation systems should be developed and flight tested as separate programs to prove the feasibility of the concept and to demonstrate the benefits and savings discussed previously. The flight test program should include one or more limited programs, limited meaning flight test on one axis and on a non-flight critical application, such as one rudder on an aircraft with two rudders. Following the limited flight test program, it is recommended that a full, 3 axis EMAS, airplane test program be performed.

Direct drive valves probably represent the next actuation system related technology to be developed and incorporated into new aircraft. As noted previously there are several valve development programs in existence. Generally speaking these are valve hardware development programs and in most cases, little has been done to integrate them into actuation systems and/or the overall FBW FCS. The problem areas noted previously, i.e., increased signal power levels, EMI, reliability base for jam free operation and chip shear force level requirements all need further investigation, system integration studies and eventually flight test, not as individual valves in limited flight test programs, but in a total integrated flight test program. The required program would complement this program in a very positive manner.

IAP's would also complement this program in a very positive way. However, the results of currently planned programs should be available before a decision should be made. At the present time the Boeing YC-14 program probably will not be completed in time for the planned program. If the YC-14 program plans do not materialize prior to start of this program, IAP's should be re-evaluated for incorporation.

The North American Rockwell Columbus Division and Vought program on light weight, 8000 psi hydraulic systems is quite comprehensive and should produce answers to the critical questions. Therefore, it would not be of any significant benefit to incorporate a light weight hydraulic effort into the planned NASA program from a technology point of view.

Rotary actuation systems, whether electrohydraulic or electromechanical could be a part of any of the previously described programs. For instance, Bendix Electrodynamics is developing a rotary, hinge line hydraulic actuator that has a redundant, rotary direct drive valve. IAP's could also include rotary hydraulic actuators in appropriate applications such as rudder, aileron or spoilers. It is therefore appropriate that final decisions regarding use of rotary actuators be made in the early definition phase of the planned program. The appropriateness of rotary actuators are very configuration dependent and the flight test vehicle and control surface complement would have to be known and studied in some depth.

4.4.7 Summary and Conclusions

We recommend that the proposed program address advanced actuation systems since they are a key element in overall FCS development and technology. Actuation systems are the last link in the FCS chain and are the interface between the 3 and 4 channel FBW system, three hydraulic systems, generally a dual (tandem) actuator and usually one control surface. In addition, the fault tolerance, fault detection and fault isolation capabilities can, if fully expoited, significantly influence the upstream elements.

The short term solution to simplicity, high reliability, and low maintenance appears to involve use of direct drive electrohydraulic control valves. Due to their inherent simplicity and reliability, they represent a significant step toward satisfying the goals of this program.

The long term and more significant approach that is recommended is the use of electromechanical actuation systems (EMAS). EMAS benefits accrue primarily because they are the key to the all-electric aircraft in which aircraft power/energy sources are consolidated into one medium, electrical power. Rather drastic improvements occur in reliability, energy conservation and, to a lesser but quite significant extent, in cost. The key reasons for this are:

- Elimination of all hydraulic systems, components, and ground support equipment.

- Elimination of engine bleed air and bleed air systems.

- The overall efficiency of current and future state of the art electrical power systems and electromechanical actuation systems.

We recommend that actuators with direct drive valves be incorporated in any immediate Advanced Flight Control program for the following reasons:

- Direct drive valves will force a major change in overall philosophy and design requirements for actuation systems.

- Direct drive valves will probably be the next major breakthrough in hydraulic actuation system design and will probably be incorporated into 1985 to 1988 designs.

- Direct drive valves impact the FBW system due to the higher signal current levels required and the lack of fault detection and isolation within the actuator.

- The benefits of direct drive valves are:

  - Simplicity

  - Increased reliability

  - Minimized quiescent flow

- Reliability and maintainability must be addressed prior to application of the concept.

- An overall aircraft program could evaluate two or more direct drive valve designs on the different control surfaces involved.

It is also recommended that a longer term EMAS study be conducted in parallel with the electrohydraulic actuation system studies noted above. The plan would be to phase EMAS into the demonstrator aircraft on an axis-by-axis basis in the 1985 to 1986 to 1989 time frame. Early efforts are recommended in the following areas:

- Evaluation of current and proposed electrical power systems followed by a preliminary design effort in development of a recommended total electrical power system.

- EMAS application study on the demonstrator aircraft including definition of requirements, evaluation of linear vs. rotary hinge line configurations for each axis of control and force vs. velocity summing for each application. The effort would include an evaluation of the impact on aircraft structure, minimal or acceptable rework of aircraft, cost, safety considerations and provisions as well as schedule and state of the art implications.

- Determination of power switching/inverter requirements, evaluation of current and future (1985-1988) state of the art components and systems and preliminary design of candidate hardware.

4.5 Network and Parallel Data Bussing

Current airborne digital systems require a variety of communications between aircraft subsystems. The communications encompass a large assortment of signals and signal characteristics. The increasing demand for high performance and high reliability and the attendant increase in data transmissions has exposed the limitations of the conventional network.

These limitations include:

- The use of dedicated, hardwired interfaces which impose significant weight, volume and power penalties, particularly in large, distributed systems.

- The use of unique signal conversion/conditioning hardware to permit interface compatibility.

- The large variety of signal characteristics and formats in use throughout the system.

- Effective redundancy requires hardware duplication. Subsystems must interface with multiple busses for purposes of cross-strapping, enhanced reliability and reconfiguration.

- The conventional flight control system architecture is often times unique to a particular application, employs non-standard hardware and allows little freedom for growth.

The selection of a communications network for an advanced flight control system was influenced by a number of factors:

- Standard (hardware, formats and protocol)

  The potential for standardization was considered an essential qualification of the bus. Standardization would result in low cost, high reliability and industry acceptance.

- Reliability

  The reliability of the bus network must support the 10(-10)/ hour survivability of the advanced flight control system.

- Economy

  The network must be economical in terms of hardware costs, maintainability, wire weight and power.

- Bandwidth

  The network must accommodate not only the flight control system but eventually the avionics system, as well. Consequently, its bandwidth should be expandable as technology improves with a minimum impact on system architecture and operation.

- Resource Pooling and Reconfiguration Capability

  The network must accommodate the pooling of resource and be compatible with a wide range of reconfiguration strategies.

- Growth

  The network must allow for system growth with a minimum impact on system architecture and operation.

- Flexibility

  The network must be flexible and capable of accommodating a variety of system and subsystem architectures such as central and distributed, sequential or parallel processing, etc.

4.5.1 Bus Selection

Busses can be classified as serial or parallel, multiplexed or dedicated. In the interest of economy, parallel and dedicated busses were eliminated at the outset or until it was established that serial and multiplexed busses proved to be infeasible.

The bus network selected for this program employed the MIL-STD-1553B standard (Ref. 10) for the primary bus. Despite its shortcomings the 1553B bus represents a mature design, is easily, and maintained has demonstrated its flexibility in numerous applications (Ref. 8), and

- it employs standard, reliable and relatively inexpensive hardware;
- there exists a large collection of bus control and interface software;
- it is generally accepted, as a standard, by the avionics industry.

The most significant shortcomings of 1553B, in the context of a flight control system, are 1) the limited number of interconnecting terminals, 2) limited bandwidth and 3) vulnerability to single point failures.

1. Limited Number of Interconnecting Terminals

   A 1553B bus can handle, at most, 31 terminals. This limitation is the results of a) terminal coupling techniques that do not allow the handling of more than 31 terminals or b) bus protocol which allows address space for no more than 31 remote terminals. As a result, remote terminals may need to service large sets of sensors and actuators. As a consequence, a failed terminal could result in a loss of a significant proportion of the resources of the system. Perhaps the worst effect, from the standpoint of the present study, is that 1553B cannot accommodate a widely distributed system on a single bus, irrespective of available bandwidth and reliability. It is possible however,by appropriate use of repeaters on bus buffers,to eliminate the electrical constraint on numbers of terminals which can be interconnected and still maintain functional compatibility with 1553. It is not possible, however, to eliminate the protocol constraint without some modification to 1553.

The terminal limitation of a 1553 bus, while potentially a serious obstacle in implementing a widely dispersed system, was considered tolerable for the purpose of demonstrating feasibility of an advanced architecture. If feasibility can be demonstrated, subject only to this constraint, then attention can be given to modifying the capabilities of 1553.

2. Limited Bandwidth

The bandwidth of 1553B is presently specified at 1 Mhz. Any increase in this rate requires a technology improvement in the interface hardware. The present bandwidth is expected to improve as new technology becomes available. Present multiplex data bus technology offers two basic configuration options: the first of these, the bipolar, Manchester coded, wire pair electrical multiplex bus, has demonstrated data rates up to 10 Mhz. Considerable effort, however, must still be expended to guarantee its performance in a typical aircraft environment. Some of the typical problems encountered are ground loops, radiated and induced noise, amplitude variation and the cost and weight of coupling devices and wire cable. The second configuration, the optical multiplex bus, represents a rapidly maturing technology. Such a bus has the inherent capability of operating two orders of magnitude faster than the electrical bus. In addition, it provides freedom from the conventional EMI problems of noise, cross-talk and ground loops. The connectors, fiber optic cables, light emitting diodes and silicon photo diodes necessary to realize a multiplexed data bus are available.

As a consequence of these technology improvements a dramatic increase in 1553 bandwidth can be expected in the near future.

Meanwhile, bus loading estimates indicate that the present 1 Mhz data rate can sustain the proposed flight control system candidate architecture.

3. Vulnerability

The most serious deficiency of 1553B in the present context is its vulnerability to single-point failures. Such a failure can disable the entire bus. Single-point failures are caused by

- physical damage due to fire, explosion, etc.
- a terminal talking out of turn (babbling terminal)
- a faulty bus controller

Physical Damage

From data obtained from a survey of all air carrier accidents from 1964 to 1975(Ref. 7) the probability of damage to the communication system was estimated. The results showed that the probability of a damage event per hour is

- 2.4 x 10(-7) for one line
- 7.5 x 10(-8) for two lines
- 6 x 10 (-9) for a control center.

The survey assumed that no unusual precautions were taken to protect against damage. As a consequence, the effects of wire protection devices and wire separation are unknown. For the purpose of configuring the bus network it will be assumed that, due to physical damage,

- the probability of loss of a single bus is 2.4 x 10(-7)/ hour;
- the probability of loss of a single bus controller processor is 2.4 x 10(-7) hour;
- two busses can be sufficiently separated to preclude loss of both busses by a single damage event.

A Babbling Terminal

1553B incorporates several mechanisms for preventing a faulty terminal from talking out of turn, the most effective of which is the use of a standby redundant bus together with a "selected transmitter shutdown" control mode command. This command requests the designated terminal to disable the transmitter associated with the specified bus. If the bus is used in such a way that a single-point failure can cause loss of a critical function and, hence, loss of the aircraft, then it must be

demonstrated that the probability of such an event is of the order of 10(-10)/hour. To establish an order-of-magnitude reliability of a 1553 bus, a preliminary assessment was performed for this study.

Preliminary Reliability Assessment of 1553B BUS

The objective was to estimate the probability of a remote terminal talking out of turn for excessive periods of time and disabling the bus, as a result. Implementation of the 1553 bus requires that "the terminal shall contain a hardware-implemented time-out to preclude a signal transmission of greater than 800 microseconds". The intention of this is to prevent a remote terminal from transmitting excessively due to a single failure. Analysis of a typical 1553 remote terminal circuit schematic indicated that no single device failure could result in babbling. It was determined, however, that certain combinations of failures could do so. Assuming the worst case, i.e., that the first failure did not result in detection and disengagement of the faulty terminal, it was established that the probability that a single remote terminal will babble as a result of two failures in a one hour flight is of the order of 3.9 x 10(-12). This analysis used failure rates from MIL-HDBK 217C, at 125 degrees C, uninhabited environment. Accordingly, the probability of at least one of 31 remote terminals babbling is 1.2 x 10(-10) per hour of flight.

It is emphasized that these estimates are based on a preliminary analysis of the terminal circuits and, consequently, should not be accepted as definitive. It will be proposed, subsequently, to corroborate these estimates by a detailed and comprehensive evaluation, as a follow-on to the present program. The suggested approach is to emulate the bus, bus controller and remote terminal at the gate-level, including the bus controller and remote terminal software.

The above estimates did not account for the possibility of disengaging the babbling terminal via the terminal shut-down procedure provided by 1553B. Using this procedure the bus would be dual, with the second bus being in a standby (i.e., listening) mode. Using a round robin strategy, the bus controller would direct each RT on the standby bus to shutdown its associated RT which interfaces with the babbling bus. The errant terminal is identified when the babbling stops, following a shutdown.

The effect of this procedure will be to improve the bus reliability by many orders of magnitude beyond the 2.34 x 10(-10)/hour cited previously. Thus, it would appear that the probability of a babbling terminal disabling a dual-bus is remote relative to 10(-10)/hour. In this connection we should note that one authority (ref. 7) cites an example of a single failure that actually occurred in the field and disabled an entire dual-bus system. Time did not permit an anlaysis of this event but it clearly establishes the need for a comprehensive study of the failure mechanisms of the 1553 bus.

Faulty Bus Controller

The most serious and critical failure event of a 1553 type bus structure is a failure of the bus controller or its associated bus interface hardware. Such an event has a relatively high probability of occurrence and could disable the entire bus. The conventional solution is to employ a combination consisting of

- bus controller self-test
- an independent bus monitor/standby bus controller.

In a typical scenario the standby bus controller assumes command of the bus if it receives a NO GO discrete from the active bus controller. This discrete can be activated by one of several failure conditions such as

- time-out of the watchdog timer,
- loss of power,
- inability to execute, pass, or complete self-test.

In addition, the bus monitor can monitor the active bus directly and request the active bus controller to relinguish control when a failure condition is detected. This approach, while effective in extending the operational life of the bus, is not likely to result in a bus controller reliability of the order of 10(-10)/hour.

In summary, the most serious deficiency of a 1553 bus from the standpoint of the objective of the Advanced Flight Control System, is its vulmerability to single point failures, in particular, to failures of the bus controller.

4.5.2 Bus Network Selection

In addition to the considerations discussed previously, the selection of the bus network for an Advance Flight Control System was motivated by the realization that the design, development and evaluation of a new bus and bus network was not a practicable venture. Considering that MIL-STD-1553 has been in development for a decade, prognosis for success and eventual industry acceptance of a new bus/bus network was not encouraging. As a consequence of these considerations, 1553B was selected as the primary communication bus and the recommended bus network is, essentially, a dual (triplex, if necessary) 1553B bus which interconnects all of the critical and redundant subsystems comprising the flight control system. It was realized, however, that the vulnerability of 1553B would have to be overcome before this approach could be justified.

An Ultrareliable Bus Controller

In the absence of a reliable bus controller the network design must incorporate redundant and independent busses. This is the classical solution to the data transmission problem. Typically, the flight control computers function as bus controllers for critical signals, directing traffic on independent and dedicated communication links. The resultant redundancy management strategy demands that remote subsystems such as sensors and actuators interface with redundant busses.

The availability of an ultrareliable bus and bus controller greatly simplifies the communications problem. Postulating such a bus, it is now possible to interconnect the entire flight control system to a single bus and still achieve the requistie survivability. If the capabilities of the bus controller were expanded it could

- service and control bus traffic;
- monitor redundant signals transmitted on the bus;
- maintain system fault status;
- manage reconfiguration by reallocating resources and bypassing faulty subsystems;
- supply an accurate clock to all subsystems.

Essentially, the recommended bus controller is a SIFT-like, fault-tolerant multiprocessor which controls data transmission throughout the system. Because of bandwidth limitations, it may be necessary to introduce multiple busses particularly if it is desired to include the avionics system, as well. The resultant bus network is shown in Figure 14. It is noted that the network does not necessarily preclude a hierarchical bus structure, i.e., dedicated and essentially private communication may be employed by a subsystem.

Interface for Bus Control

Initially, a set of redundant processors is assigned control of a bus but only one processor actually controls the bus at any given time. The other processors monitor the active bus controller by continually listening to the bus transactions. When a fault is detected and attributed to the bus controller by a majority vote, the faulty controller is physically disengaged from the bus and an alternate is engaged. This is accomplished by means of an independent switching network which is functionally equivalent to a multiplexer. The multiplexer address is supplied by majority logic from the multiprocessors. A functional schematic of the interface for bus control is shown in Figures 15 and 16.

Referring to Figure 15, the active bus controller controls a "local network" consisting of a dual bus, one of which is a standby, and continues to do so until it fails. Bus switching is effected by two, tandem switches one of which is activated by the associated processor (the isolator in Figure 16 is set to a high impedance state) and the other by hardwired logic to the multiplexer. A monitoring processor would, nominally, be disengaged from the bus by both switches, but in the event of a failure of either switch it would remain disengaged.

We note that the bus interface hardware could be used to implement other types of bus networks, if desired, e.g., the busses could be grouped into triads of independentcy controlled and continuously active busses instead of the active/standby arrangement favored here.

Interface for Bus Monitoring

There are three candidate configurations for bus monitoring.

Configuration #1 (Recommended)

This arrangement is shown in Figure 17. In this configuration a processor can listen to any pair of busses, simultaneously. When a triad of processors has been assigned control of a network, one processor will function as bus controller and the other two will select the network for listening.

- Advantages
  - only two extra receivers on the network (in non-failure case)
  - direct listening
  - minimum number of receivers
  - no restriction on triad membership
- Disadvantages
  - a processor can only listen to two busses, simultaneously
  - requires additional multiplexers

Configuration #2

This arrangement is shown in Figure 18. In this arrangement any processor can listen to one or more local networks simultaneously.

- Advantages
  - direct listening
  - a processor can listen to all networks
  - no restriction on triad membership
  - no bus switching logic for listening
- Disadvantages
  - adds a terminal for each processor

Configuration #3

This arrangement is show in Figure 19. In this arrangement any processor can monitor one or more bus transaction, but not directly, as in the previous configuration.

- Advantages
  - a processor can listen to all bus transactions
  - no restriction on triad membership
  - no bus switching logic for listening
  - no extra network terminals
- Disadvantages
  - requires extra receivers and intercomputer data links
  - indirect listening

4.5.3 Summary Properties of Bus Network

1. Network Architecture

   The bus network consists of a set of local networks, each consisting of at least a pair of 1553B busses. Each bus may be assigned a separate function such as flight control, avionics, engine controls, etc. At least one local network will be dedicated to flight controls and will interconnect all of the necessary, critical and redundant subsystems which comprise the flight control function.

2. Ultrareliable Bus Control

   The local networks are controlled by a fault-tolerant, multiprocessor system which performs the following functions:

   - services and controls bus traffic
   - monitors redundant signals transmitted on the bus

- maintains system fault status
- manages reconfiguration by reallocating resources and by-passing faulty components
- supplies an accurate clock to all subsystems

We note that the bus controller is essentially a passive device, i.e., except for the clock it does not transmit data to any subsystem. Thus, a malfunctioning bus control will, in the worst case, suspend communications unil it is replaced.

3. 1553B Busses

Each local network consists of a least two 1553B busses, one of which is a standby. The pertinent (from the standpoint of this study) characteristics of the bus are:

- 31 terminals, maximum
- 960 distinct labels
- 30 distinct messages
- 1 mhz bit rate
- maximum error rate = 1 word in 10(7) (Ref. 10)
- undetected bit error = 1 bit in 10(-12) (Ref. 10)
- probability (estimated) of a babbling terminal is less than 3.9 x 10(-12)/hour
- probability of one of 31 terminals babbling is less than 1.2x 10(-10)/hour, exclusive of the use of a shut-down procedure
- standby bus (if available) can be used to shut-down a babbling terminal
- expandable to a fiber optic bus @ 20 mhz
- can accommodate synchronous and asynchonous computations
- transparent to application processors

4.6 FIBER OPTIC COMMUNICATION MEDIA

1. Current State of the Art in Electro-Optics

Present multiplex data bus technology offers two basic system configuration options. The first of these, the bipolar, Manchester coded, wire pair electrical multiplex bus, has been described and built numerous times. While it performs adequately in systems with data rates up to 10 Mhz considerable effort must be expended to guarantee its performance in typical aircraft environments. Some of the specific problems encountered are ground loops, radiated and induced noise, amplitude variations and the cost and weight of coupling devices and wire cable.

In contrast, the optical multiplex bus, represents an inherently powerful, rapidly maturing technology. Although MIL-STD-1553B specifies a data transfer rate of 1.0 Mhz, this system has the potential of operating two orders of magnitude faster. In addition, it provides freedom from the conventional EMI problems of noise, cross-talk and ground loops. The connectors, fiber optic cable, light emitting diodes and silicon photodiodes necessary to realize a military multiplex data bus system are available now.

Other significant advantages of fiber optic cable are its excellent radiation resistance and low weight. Typically, fiber optic cable weighs only one-tenth as much as its copper counterpart.

Problems associated with fiber optics include cable cost, terminations, losses in multiport systems and vibration. While typical prices of fiber optic cable are 3 or 4 times that of conventional cable, part of this is offset by easier installation. For airborne applications, the lower weight increases range and/or payload capability. This, also, results in a cost saving. It is anticipated that, as fiber optic cable is manufactured in greater quantities, the prices will decrease significantly.

Coupling losses are encountered in two areas. First, the small diameter of fiber optic cables required precision-made connectors and terminations which must be ground and polished correctly to minimize coupling losses. Second, multiport systems result in losses which are minimized by the selection of optimum coupling devices (e.g.-star couplers). In addition, the losses are compensated for in the design of the electro-optic transmitters and receivers.

While various fiber-optic systems have been flight tested successfully, information on long term exposure to shock and vibration is required. This information will permit the development of appropriate techniques for fiber optic cable and harness installation in the aircraft environment.

A survey of the current generation of electo-optic cables and interface components shows a wide selection of devices. Low loss cables for transmission over distances in excess of 50Km are available. Emitters, detectors and support electronics for the transfer of data at clock rates of 100 Mhz and higher are also available. The only limitation, at present, is that there are few systems specified for operation from -55 degrees C to +125 degrees C.

2. Fiber Optic Bus Feasibility and Performance

Replacing the 1553 bus by a fiber optic equivalent is not only feasible but has been demonstrated several times. One of these fiber optic replacement systems operated at a data rate of 10 Mhz while preserving the 1553 protocol and formats. Fiber optic links to digital flight control, computer peripheral and air data computer systems have been flight tested. The military committment to electro-optics is underscored by a wide range of bus oriented study and hardware development programs. Wright Patterson's microelectronics branch has developed its own transmitter and receiver chips for data transfers to 10 megabits per second.

Bit error rates in electro-optic systems are a function of the signal-to-noise ratio present at the input to the receiver. Therefore, a bit error rate is selected during the design of a system as a function of the data rate, emitter, detector and temperature requirements.

The bit error rate is usually chosen to be approximately 10(-8) to 10(-9). These values do not appear to pose a problem in a 10 Mhz system.

3. Technical Forecast

The development of a 10 Mhz, 1553 style, fiber optic data bus will alleviate the increasing bus congestion in the 1 Mhz systems of today. However, with the proliferation of distributed processing, the growing complexity of avionics systems and the demand for greater reliability in these systems, it is extremely probable that, in 10 years, we will find ourselves chafing at the restrictions imposed on us by a 10 Mhz bus rate. The history of electronics has shown that as our capabilities increase so does our utilization of these capabilities. This, in turn, generates the need for even greater capabilities. One advantage of electro-optics is its inherently large bandwidth. This will allow an easier transition to even higher data transfer rates than would be possible in a solely electrical configuration.

4.7 INTEGRATED SENSOR TECHNOLOGY

4.7.1 Introduction

Integrated sensor technology for advanced aircraft applications is being studied by the Air Force and the Navy. These programs were reviewed and a brief description of each program is included in this survey. Table 1 contains a summary of the characteristics of the different approaches and a statement of the developmental status of the program. A description of the recommended sensor configurations is given in Appendix D.

4.7.2 Integrated Sensor Configurations

1. Quad In-Line

   The most direct approach to obtaining two fail-op redundancy for inertial sensor data is to use quad redundancy. For flight control application this requires twelve (12) gyros; four (4) per axis aligned with the aircraft pitch, roll and yaw axes, as well as eight (8) accelerometers, four (4) each for the measurement of normal and lateral accelerations. These redundant sensors can be readily dispersed for survivability by the application of state estimation techniques. The state estimation is used to remove the aircraft bending kinematic acceleration effects which may differ at different sensor locations.

   For AHRS applications, the quad redundant approach will require twelve (12) gyros and twelve (12) accelerometers of higher quality than the flight control application. For navigation functions, the same number of sensors is required; however, they must be of inertial navigation quality with the attendant high cost per sensor.

   The redundancy management, including fault isolation, for the quad-redundant sensor set can be performed in dedicated microprocessors or integrated into the flight control computers. Redundancy management algorithms have been developed for the three computer and four computer configurations.

2. Integrated Sensory System (ISS), Single Degree of Freedom (SDOF) Gyro Configuration (Reference 22)

   The ISS is composed of three elements. The first is a sensor set consisting of hard-mounted skewed and dispersed rate integration gyros and accelerometers, low and high speed air data probes (which are planned to be located in close proximity to modularized

air data transducers) an Inertial Navigation System, pilot command sensors, surface and engine position transducers, and a set of radio navigation devices and landing aids. The second element is a reliable and survivable input-output (I/O) system that links the data from the redundant sensors to redundant flight control computers. The third element is a group of computational subroutines that reside within the redundant computer complex, which performs the various data handling functions such as redundant data management, "best" estimate and output parameter computations.

The inertial sensor set consists of six SDOF gyros and six accelerometers with the input axes arranged in cone configurations as shown in Figure 20. The inertial components are medium grade types of instruments (i.e., gyro accuracy = 10 degrees/hr.; accelerometer accuracy ≃ .002g). In addition to body rate and acceleration data utilized for inner loop FCS functions, the inertial instruments provide the reference data for computer attitude and heading.

The two fail operational inertial sensor set is packaged into three Inertial Component Assemblies (ICA) which are dispersed, as shown in Figure 21 to assure a survivable sensor system.

Each ICA contains two gyros, two accelerometers and associated interface electronics. State estimation algorithms contained in the data handling software are used to remove dissimilar body bending and kinematic effects that are sensed by the dispersed ICA's.

3. ISS - Two Degree of Freedom (TDOF) Gyro Configuration

The ISS skewed inertial sensor cone configuration can be implemented with TDOF gyros. This configuration has two TDOF gyros and 3 accelerometers in each of two Inertial Reference Assemblies (IRAs). The gyro input axes are configured on a 45 degree cone with its axis along the aircraft roll axis as shown in Figure 20. The accelerometers form a cone identical to the SDOF ISS configuration when the IRA's are installed as shown in Figure 22.

The rate and acceleration outputs from the two IRS's are fed to each of the three computers in a redundant flight computer set in a similar manner to the ISS SDOF configuration. The sensor redundancy management is performed in each of the computers and the results interchanged and compared between the computers.

4. IISA (Integrated Inertial Sensor Assembly) (Reference ??)

The Integrated Inertial Sensor Assembly Advanced Development Model (ISSA-ADM) is an integrated reference and navigation system using Ring Laser Gyros (RLGs) in a strapdown configuration. The primary objective in the design of this assembly is to provide a navigation, flight control and weapon delivery capability with a lower cost avionics system which satisfies the performance, redundancy management and physical requirements of advanced aircraft applications.

The IISA would be comprised of two Inertial Sensor Assemblies (ISAs), and two Digital Computer Assemblies (DCAs) (see Figure 23).

The ISAs would contain a sensor array consisting of three RLGs, three accelerometers, navigation electronics, and flight control electronics. Each ISA shall be rectangular in shape and aligned with the aircraft axes to simplify installation. Within each unit, the three sensor axes shall be held orthogonal with respect to each other but skewed with respect to the aircraft axes. The sensor array shall be mounted so that each sensor axis is at an angle of 54.7 degrees with respect to the aircraft yaw axis. The two ISAs shall be mounted in the aircraft with a 180 degrees rotation between them so that no three of the six sensor axes are coplanar. As a result, the redundancy level for flight control shall be equivalent to a hexad sensor array.

Each of the two DCAs shall contain two independent flight control processors, electronics, and one navigation processor. The DCA redundant electronics in conjunction with the hexad sensor array shall provide a fail operational/fail safe fault tolerance capability for flight control inputs. The ISAs shall output redundant flight control (FC) sensor data to both DCAs. The navigation information shall be independent from each of the other respective IISA channels.

The skewed sensor redundancy management including fault detection is performed in the dual flight control processors contained in each DCA.

5. Multi-Function Inertial Reference Assembly (MIRA) (Reference 24)

The MIRA configuration is a single line replaceable unit (LRU) as shown in Figure 24 which contains the redundant inertial sensors and associated electronics. The inertial sensor assembly contains either four two-degree-of-freedom tuned rotor gyros (TRG) or five single-degree-of-freedom tuned rotor gyros (TRG) or five single-degree-of-freedom ring laser gyros (RLG) and five accelerometers. The inertial sensors are high accuracy instruments to perform the navigation functions in addition to providing FCS stabilization data.

MIRA has five sensing vectors, as shown in Figure 25. The geometry of the five sensing vectors is such that three of them are aligned with the three aircraft p, q, and r axes. A favorable location for a fourth axis is along the axis of a cone on whose surface the three primary axes lie. With this orientation, the fourth axis lies at a 54.7 degrees angle relative to each of the p, q and r axes. The fourth axis can thereby sense a large component relative to the other four axes. If a fixed orientation for the fifth axis needed to be defined for both TRG and RLG applicability, location could be perpendicular to the fourth axis and rotated 30 degrees about the fourth axis from the plane containing the fourth and the p axes. Gyro and accelerometer input sensing axes are mounted parallel with the five above-described directions.

Two built-in navigation microcomputers perform computations for gyro and accelerometer compensation; for alignment, coordinate transformation, navigation, flight control, built-in-test, input-output, failure detection fault isolation, fault coverage, and MIL-STD-1553A MUX bus compatibility; and for executive and sub-routine service. Two additional microcomputers perform necessary safety-of-flight control computations.

It is to be noted that the MIRA Program was a concept feasibility study performed for the Air Force. The follow-on effort, IIRA (Integrated Inertial Reference Assembly) will perform the system architectural trade-off necessary to achieve the redundancy/survivability requirements of advanced aircraft applications.

The MIRA program recommended that a flight test program be conducted to evaluate redundancy management of navigation quality ring-laser gyros and accelerometers under high dynamic conditions with particular emphasis on flight control. In May 1980, AFWAC/FI

awarded the Multifunction Flight Control Reference System (MFRCS) program contract to McDonnell Douglas Corp. for incorporation into a F-15 aircraft. The primary goal of the MFCRS program was to verify that the outputs of inertial grade sensors in a strap-down configuration can be processed by a digital computer and used as the flight control feedback reference in a modern fighter.

4.7.3 Recommendation

A review and assessment of current integrated sensor technology configurations results in the conclusion that the Integrated Sensory System (ISS), (See below) Single Degree-of-Freedom (SDOF) gyroconfiguration is the recommended candidate program for the Advanced Flight Control System Study.

This conclusion is based, in part, on a preliminary assessment of the system design and in-house laboratory and flight testing. Further technical support is required to finalize the recommended system by an in-depth review of the following associated factors:

- Reliability
  - Trade-offs
    - -- System Reliability
    - -- Safety Reliability
    - -- Design Maturity
    - -- Dispatch Reliability
- Performance
  - Effects of Environment
  - Physical Configuration, Dispersion
  - Expansion Capability
    - -- Navigation, Autoland, etc.
- Survivability
  - Dispersion
  - Commercial vs. Military

- Maintainability
  - Failure Isolation
  - Spares Requirements
  - Level of Maintenance
    -- Organizational
    -- Intermediate

The results of the above in-depth review, with proper weighting of the various factors, should result in an affirmation of the recommendation.

4.8 Multifunction Displays

The cockpit envisioned for the Advanced Flight Control System aircraft will incorporate six Cathode Ray Tube (CRT) displays that provide the means for combining large amounts of information into integrated displays. These units will be furnished with full color capability using a shadow mask CRT. Not only is the display content increased but the use of constrasting colors results in significant advantages in display information separation. Thus faster identification of data, with reduced error, is possible. This reduces the pilots overall workload.

In addition, the capability for transferring information from one display to another, inherent in the design of the system provides multiple levels of redundancy. For example, the attitude indicator (ADI) and navigation indicator (HSI) can be combined in an emergency, each providing a backup for the other.

The ADI and HSI displays (see Figure 26) are dedicated functions for the pilot and copilot. These make up four of the six displays. The remaining two units will be used in a multifunction role to display and control autopilot mode selection, warning and caution data, preflight and postflight checklists, emergency procedures, and any additional data that will facilitate the pilot's decision making ability and reduce his workload. Control of the Multifunction Displays (MFD) is achieved by means of momentary switches located around the periphery of each MFD (see Figure 27).

The required number of preprogrammed checklist, procedure, and performance data will be stored and recalled when required. The system's emergency checklists are automatically displayed when an emergency condition arises. This is also true of the warning and caution data, which appears on the display when the failure condition occurs.

The six displays provide the pilot with most of his contact with the airplane electronic systems. Display generation and the control redundancy designed into the proposed system assure the pilot's continuous awareness of and means for control of the airplane situation via its electronic systems.

Associated with these displays is a data entry panel (Figure 28) to provide the pilots with the means for manual data entry into the system. It will be used primarily for preflight checkout and system calibration. In flight, mode selection and other pilot functions will be performed through the switches on the MFD's.

Each display is a 5 inch by 5 inch full color, shadow mask CRT unit. Each has the capability of being driven in stroke, raster or raster/stroke overlay modes. Two of the displays will have twenty push buttons and four rocker switches located around the periphery of the unit for mode control and display selection. Fifteen of the push buttons are encoded internally and transmitted to the processor via a dedicated broadcast data link. The remainder of the push-button outputs are available for use by the processor or by other external equipment. A Block Diagram of the display unit is shown in Figure 29.

Phosphor protection circuitry is provided in each display unit. It monitors power, CRT bias voltage, and sweep. A failure will inhibit beam current to prevent permanent damage to the CRT.

The control unit, shown on the bottom section of the display (Figure 27) contains the display power switch, brightness, contrast, and balance controls and can be remotely located if desired. Pertinent physical and electrical characteristics of the display unit are presented in Table 6.

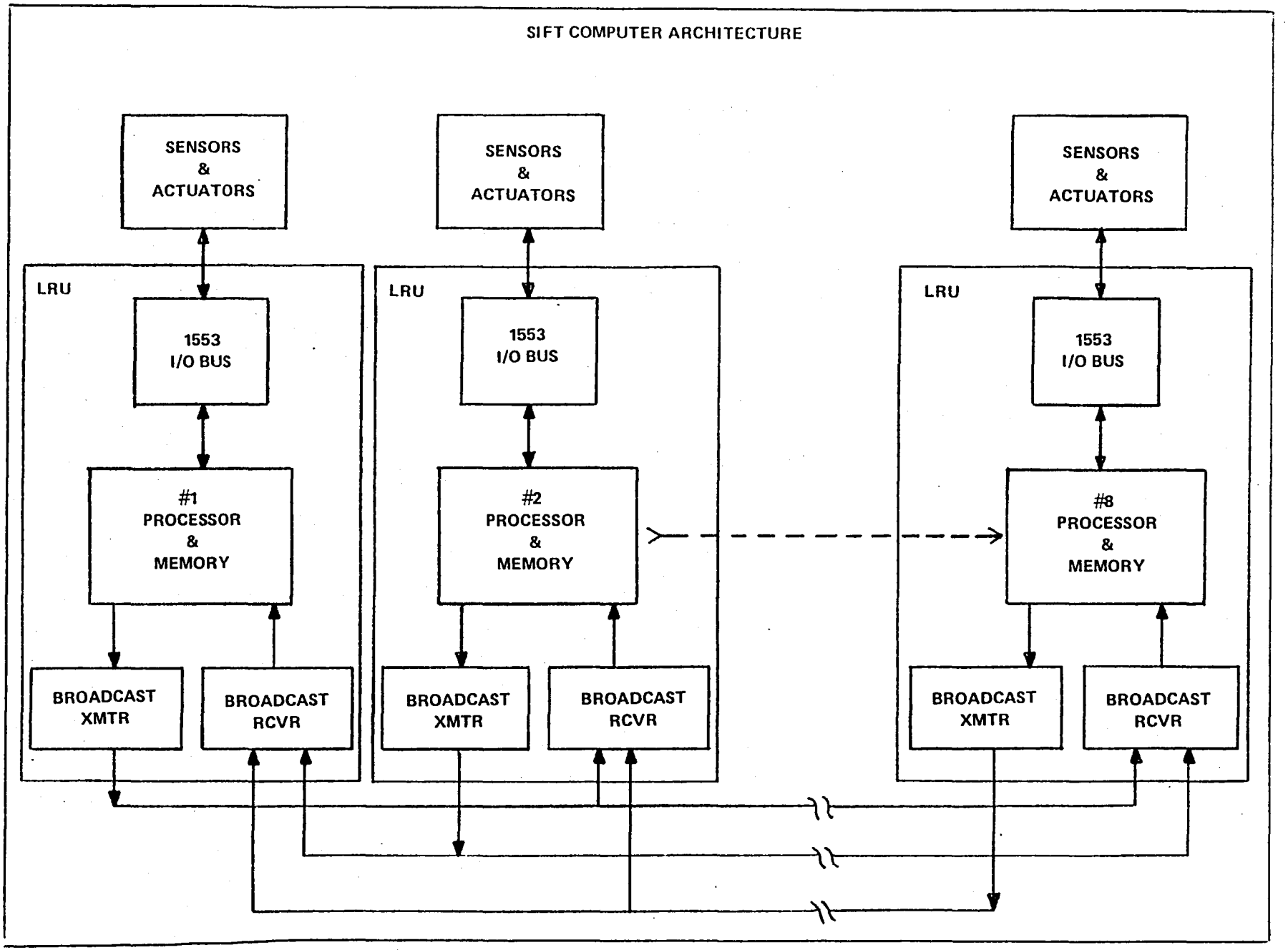


Figure 2 Serial Broadcast Busses

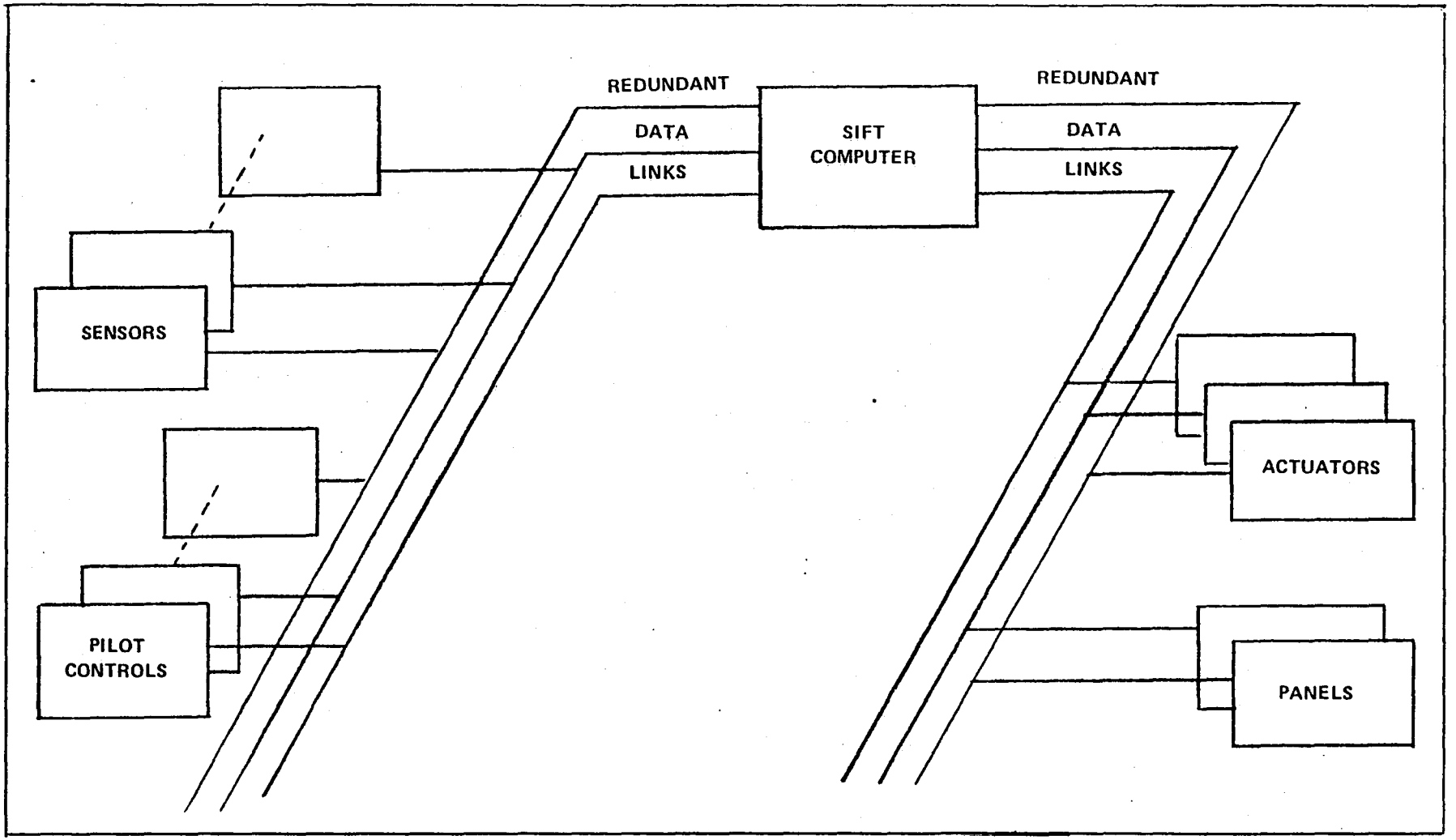


Figure 3 Architecture Fully Integrated System

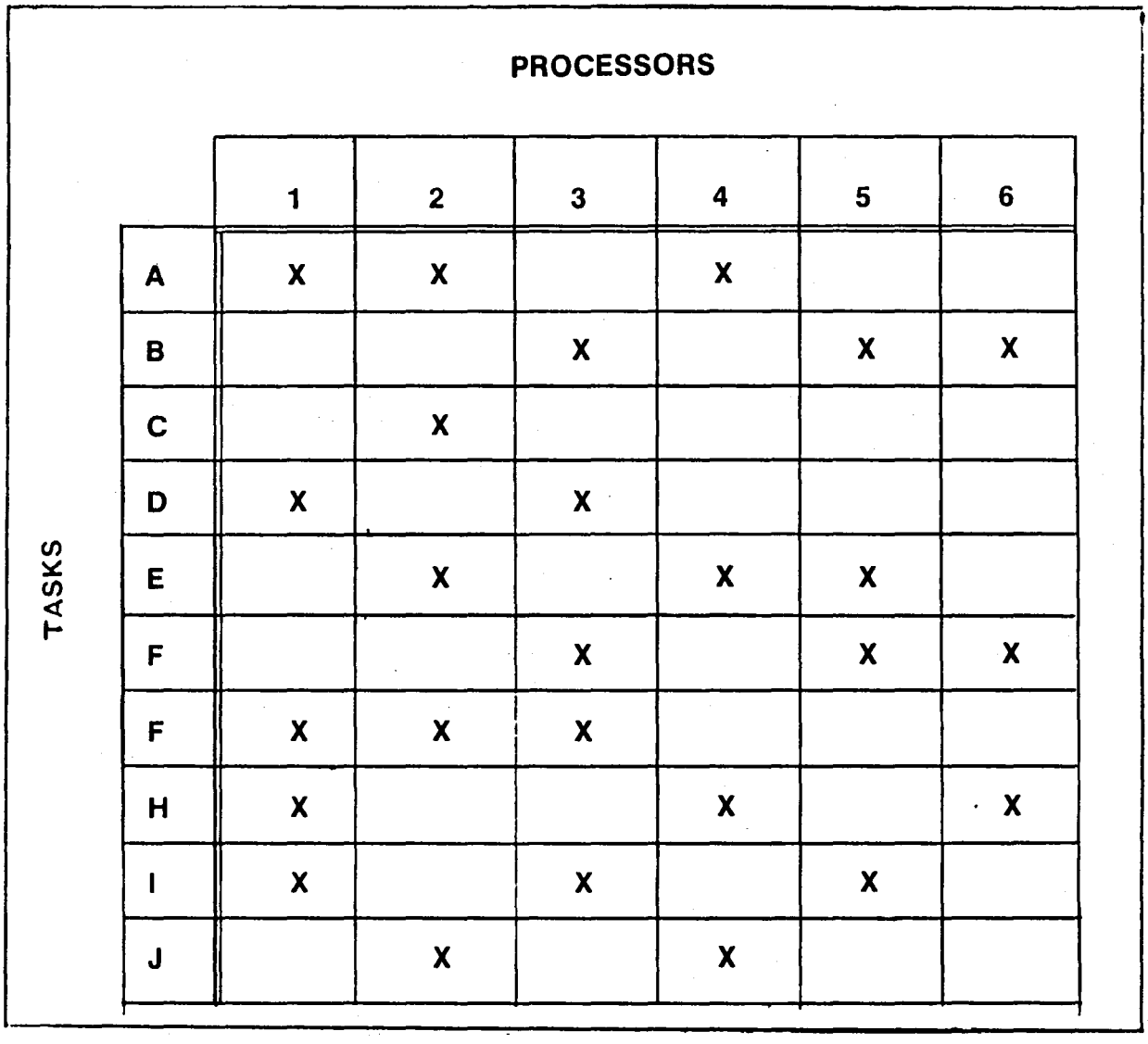


Figure 4 SIFT Typical Task Distribution

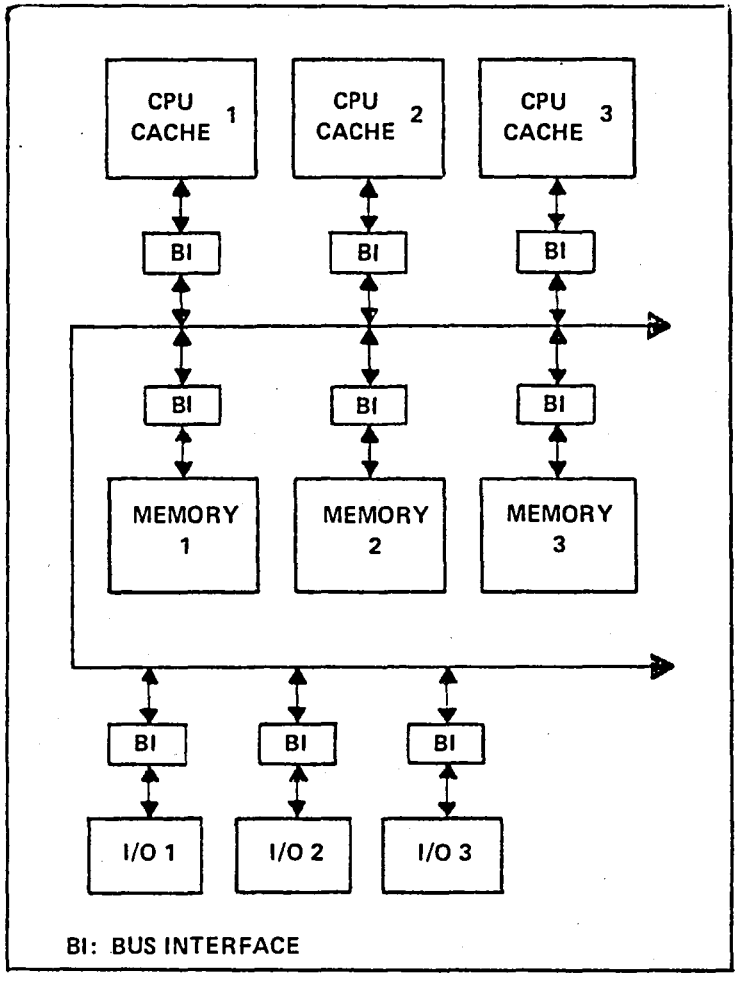


Figure 5 FTMP Physical Organization

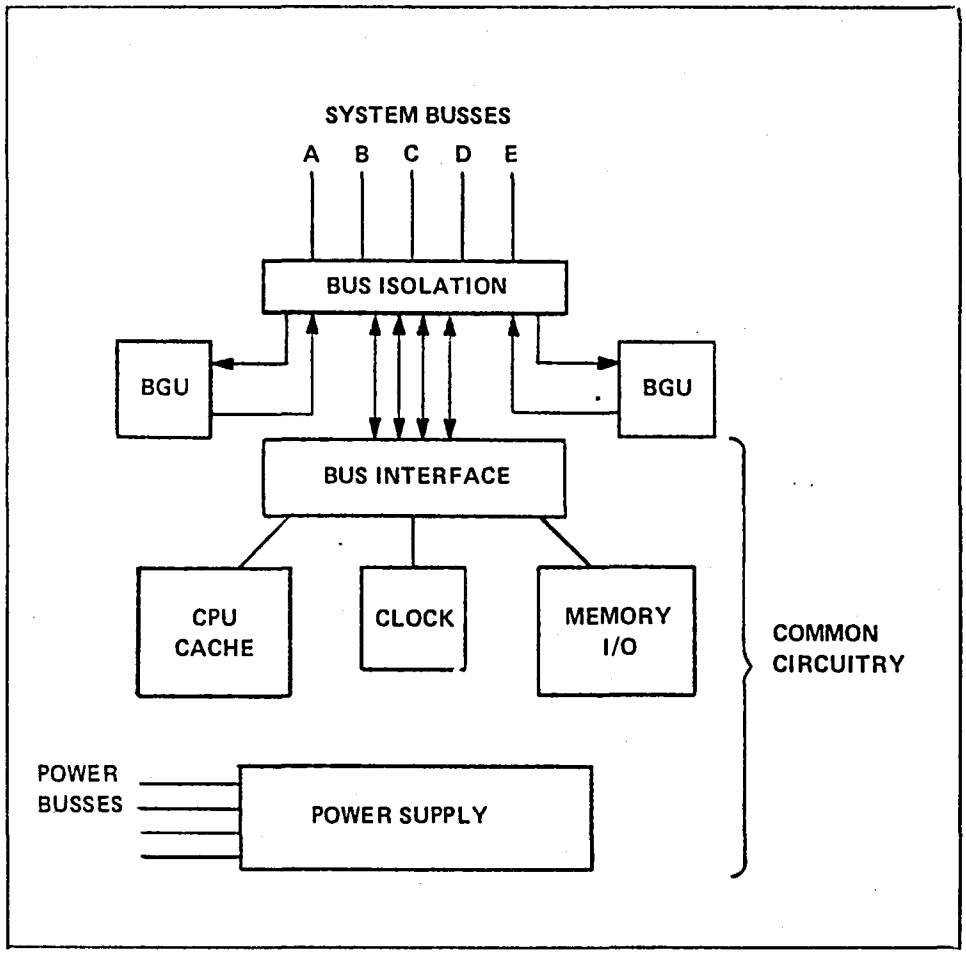


Figure 6 LRU Block Diagram

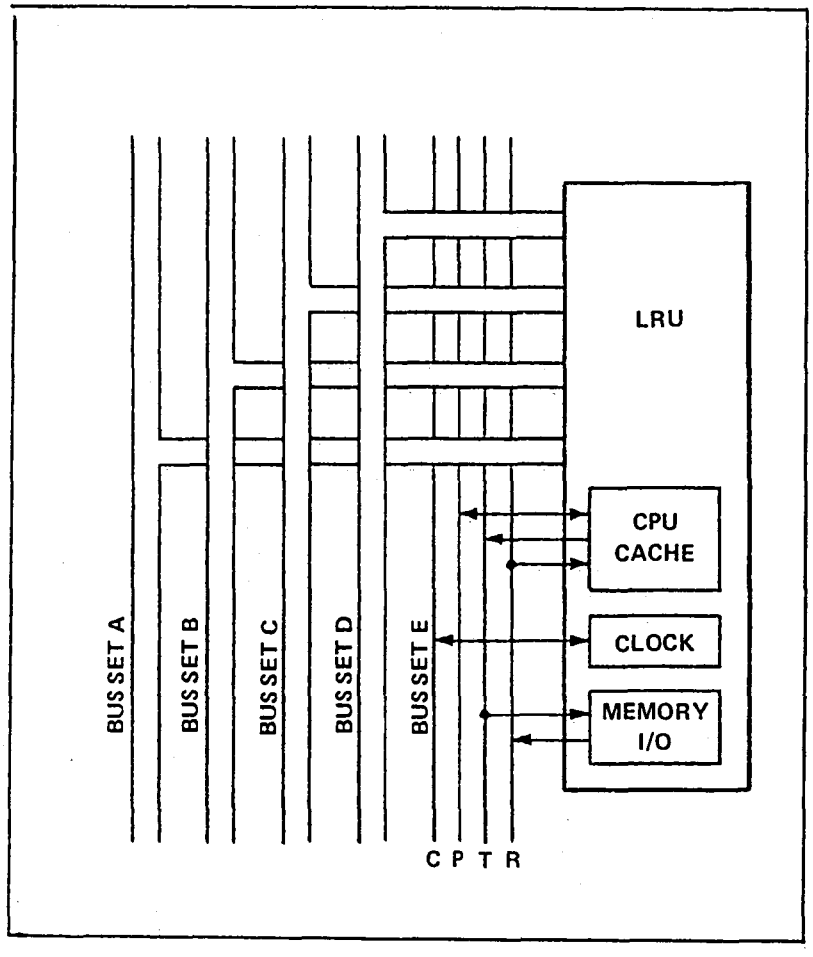


Figure 7 LRU and Bus Interconnections

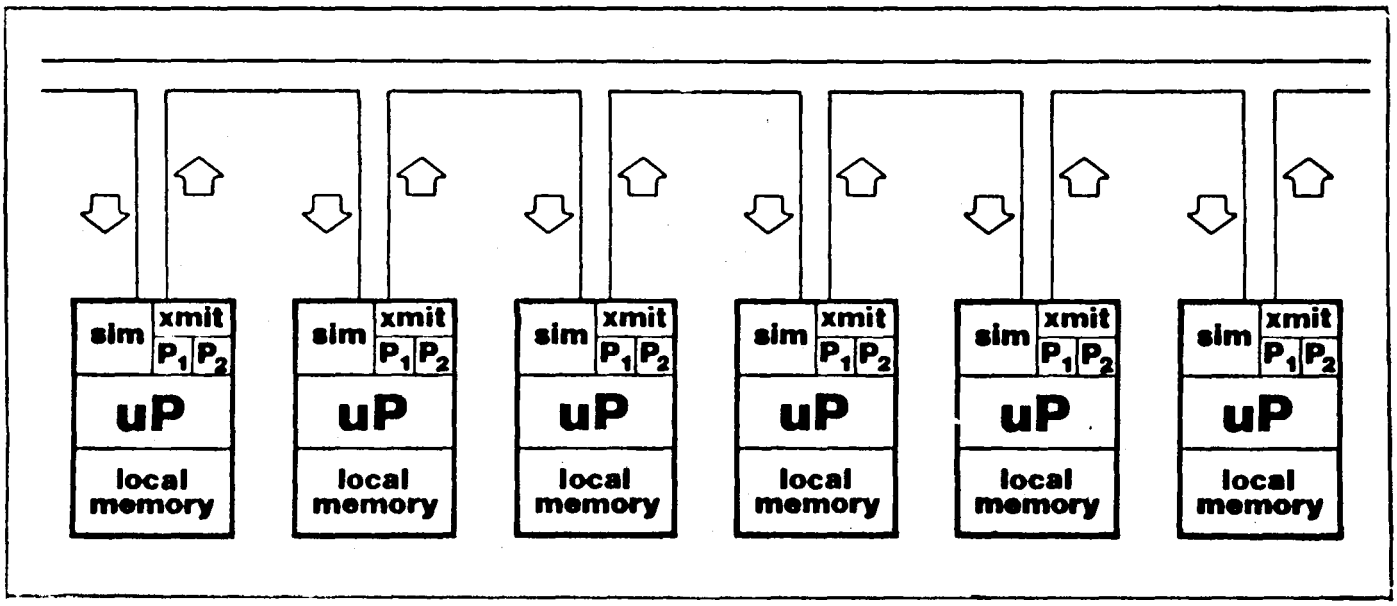


Figure 8 Virtual Common Memory Continuously Reconfiguring Multimicroprocessor

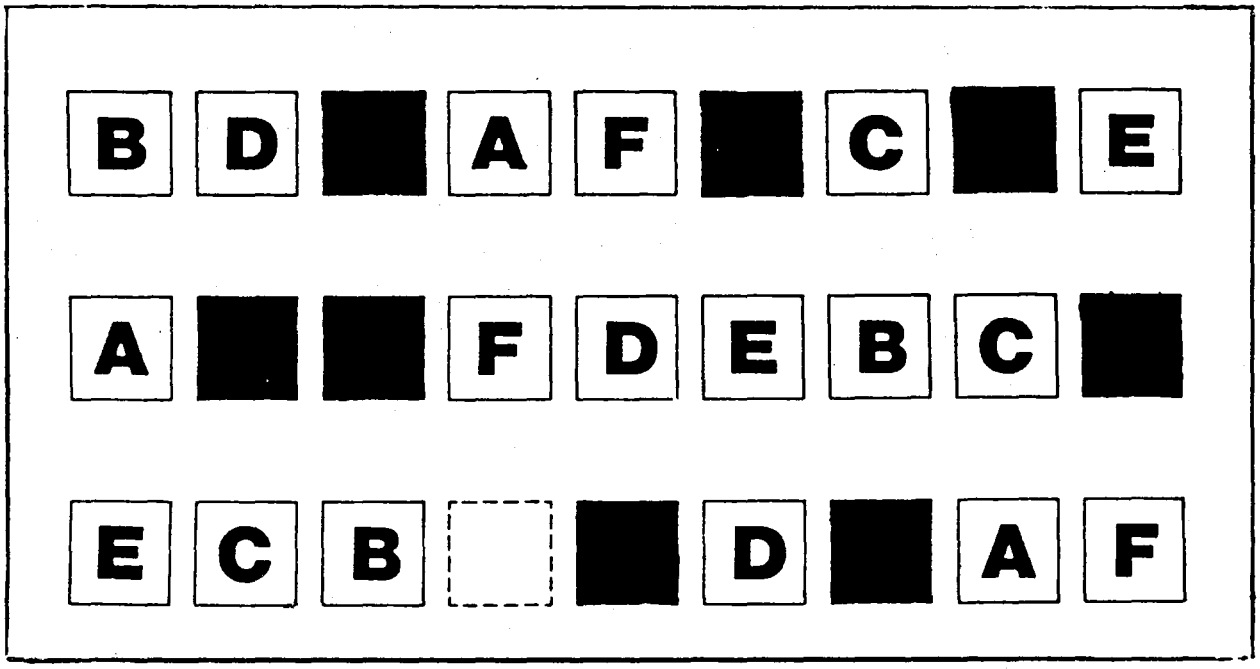


Figure 9 Continuous Reconfiguration

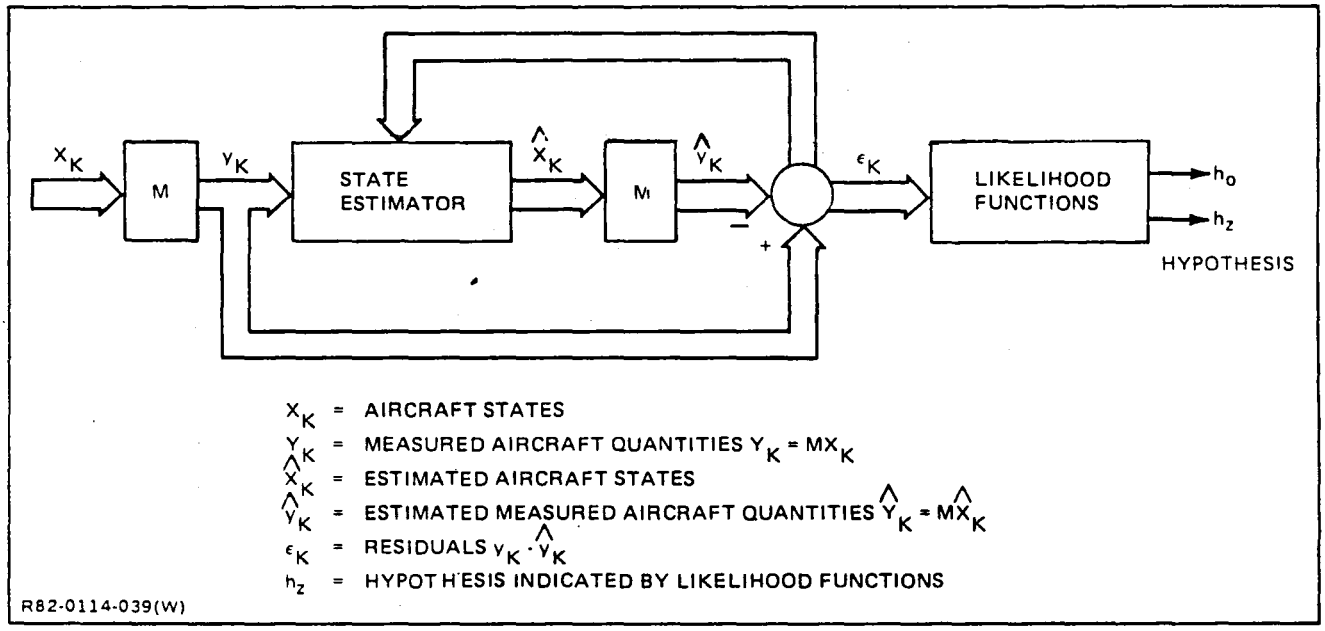


Figure 10 Generalized Likelihood Fault Detection Scheme

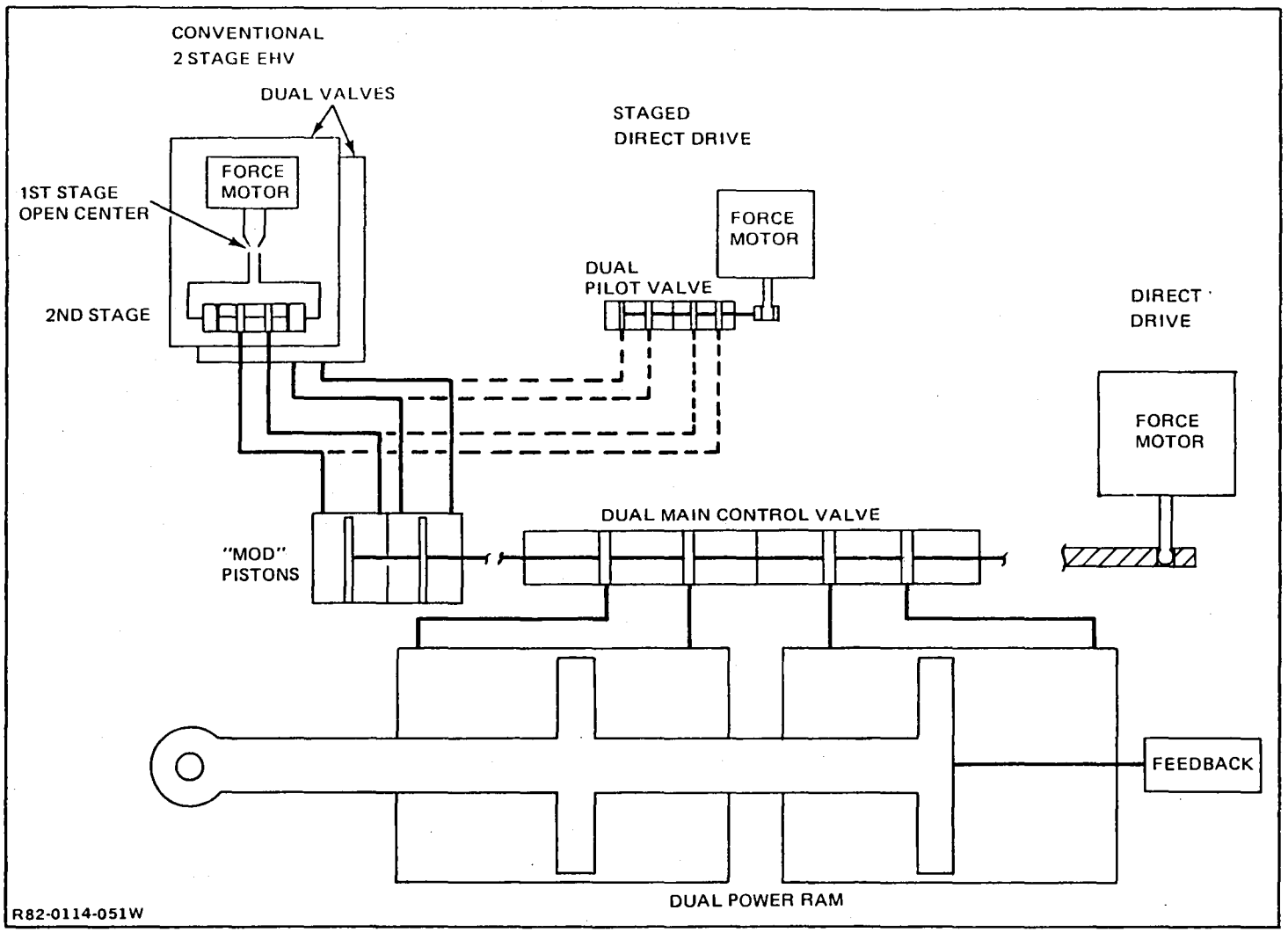


Figure 11 Valve Drive Comparisons

PROGRAM	STROKE (IN.)	FORCE OUTPUT (LB)	FLOW (GPM)	POWER INPUT (W)	CONFIGURATION	APPLICATION REFERENCE
ROCKWELL INTL NADC	±0.040	40	5 (8000 PSI)	32 (TOTAL)	DIRECT DRIVE	T-2C RUDDER
DYNAMIC CONTROLS AFWAL	±0.014	80	14	64 (TOTAL)	DIRECT DRIVE	F-4 AILERON
GENERAL ELECTRIC AFWAL	±0.066	80	14	26	DIRECT DRIVE	F-4 AILERON
MCAIR/LEDEX AFWAL	±0.060	60	15	120	DIRECT DRIVE & STAGED DIRECT DRIVE	F-15 (FBW) STABILATOR
ROCKWELL INTL MOOG NADC	–	>50	4 (AT 3000 PSI) (8000 PSI SUPPLY)	100	DIRECT DRIVE	T-2C RUDDER

R82-0114-067W

Figure 12 Direct Drive Valve Programs Principal Characteristics

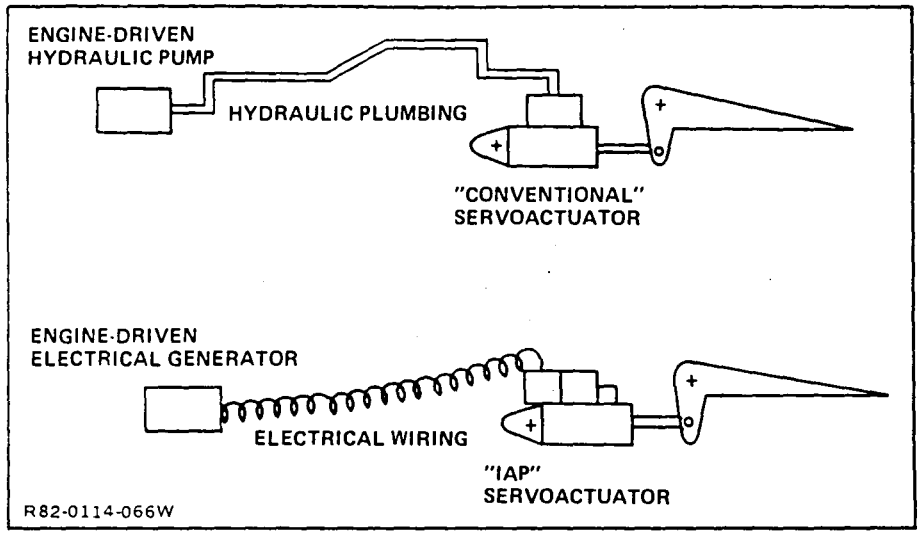


Figure 13 Integrated Actuator package (IAP)

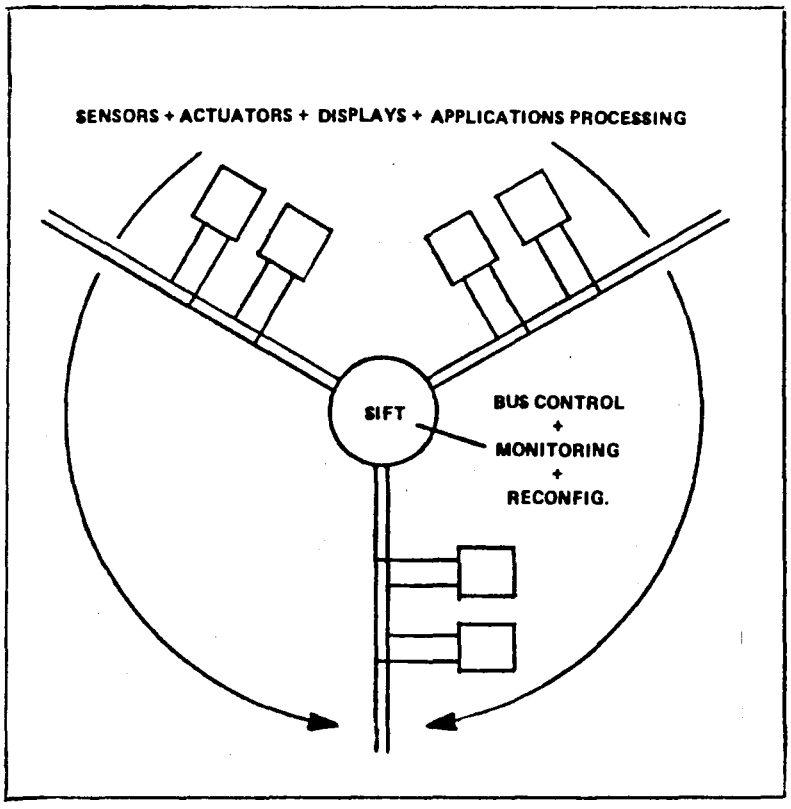


Figure 14 Candidate Bus Network

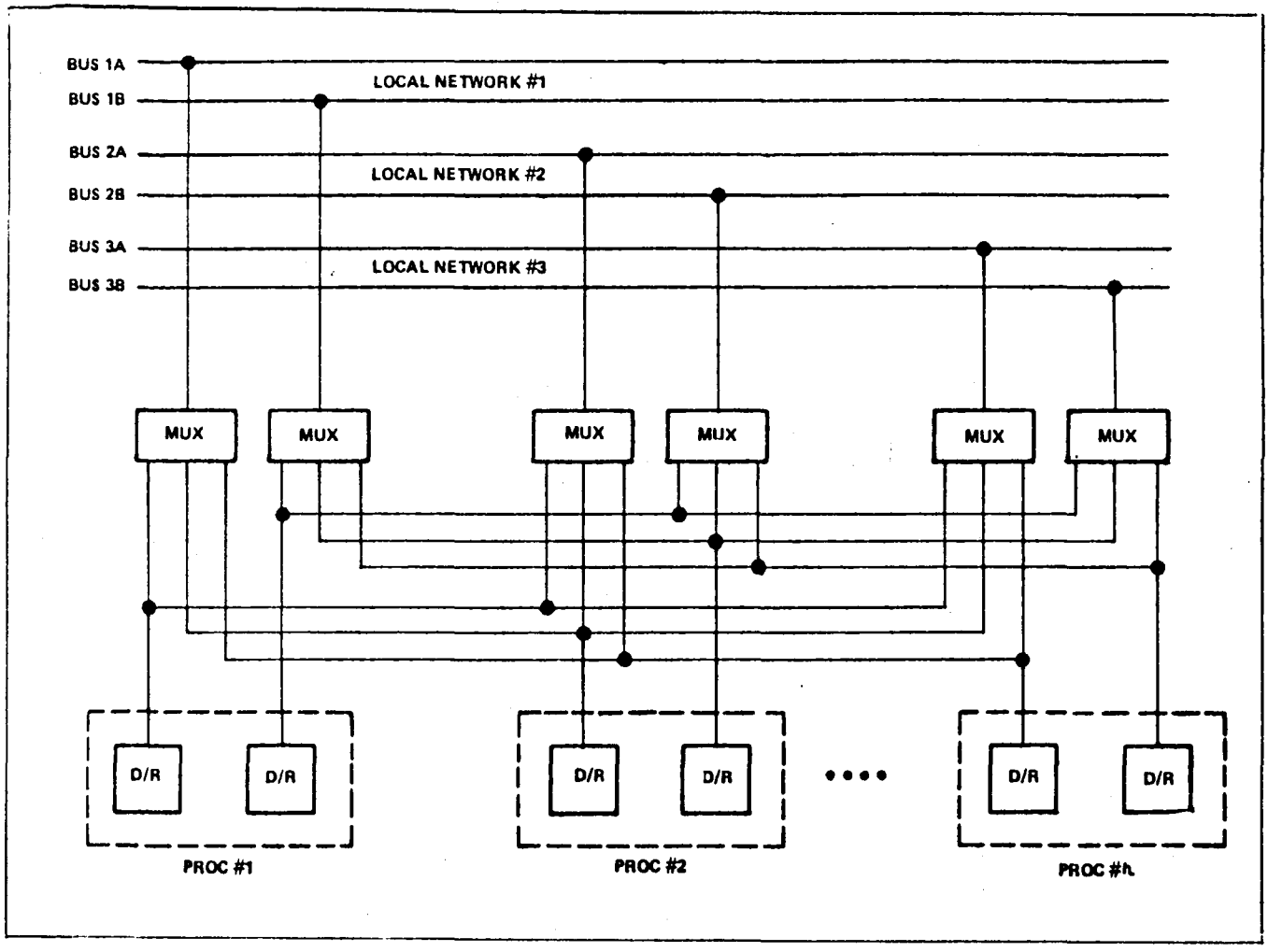


Figure 15 SIFT/1553B Interface for Bus Control

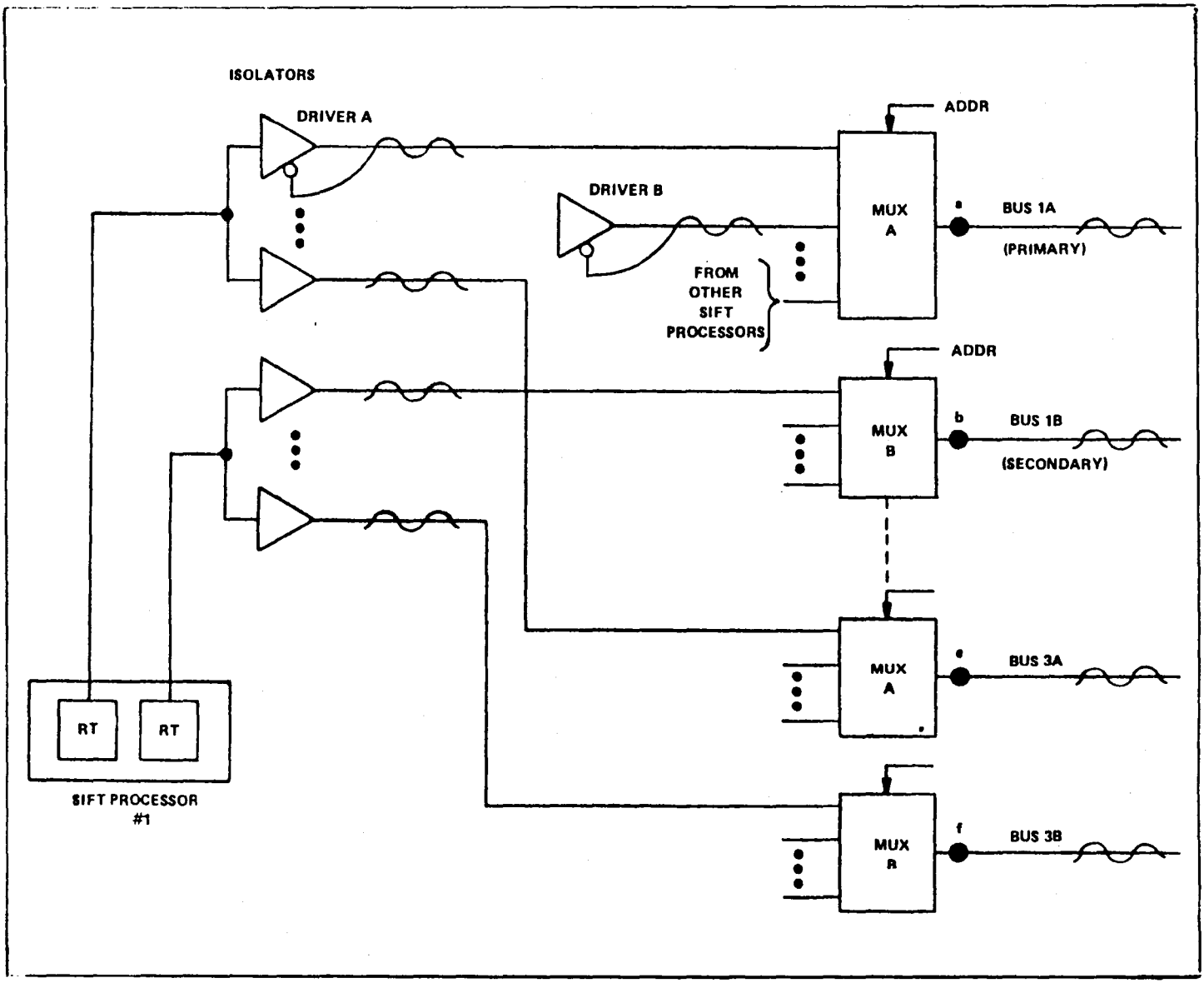


Figure 16 Recommended Bus Switching

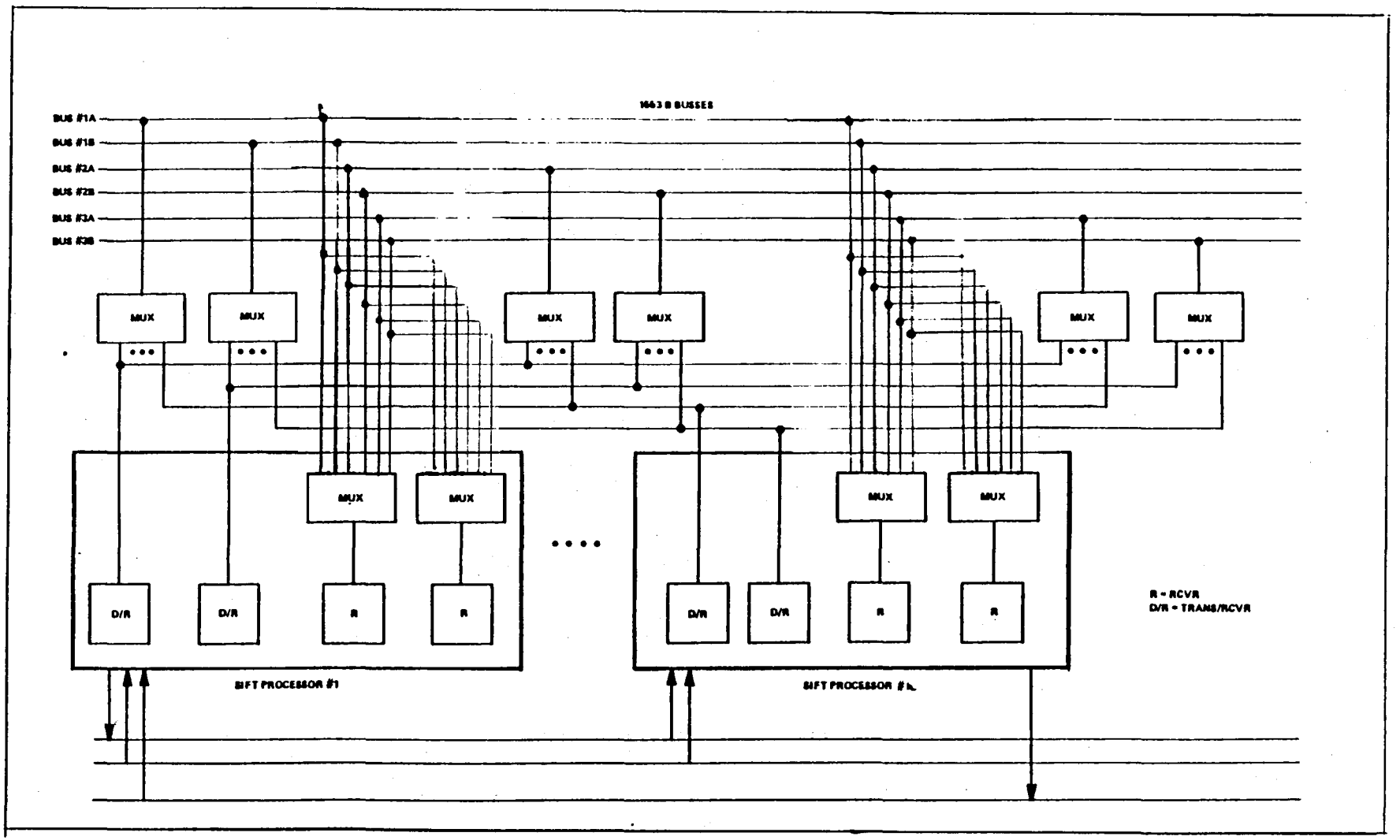


Figure 17 SIFT/1553B Interface Configuration # 1

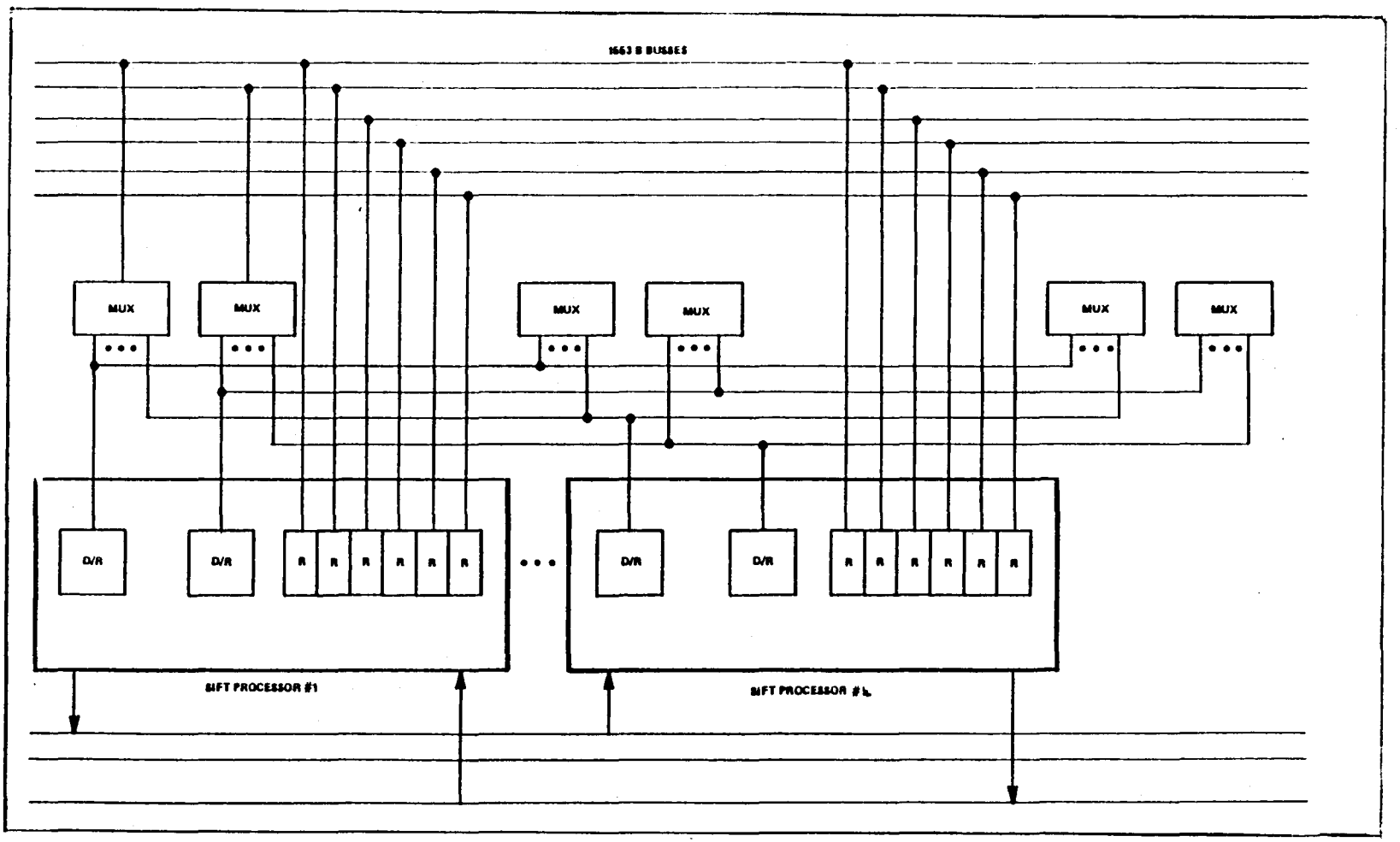


Figure 18 SIFT/1553B Interface Configuration # 2

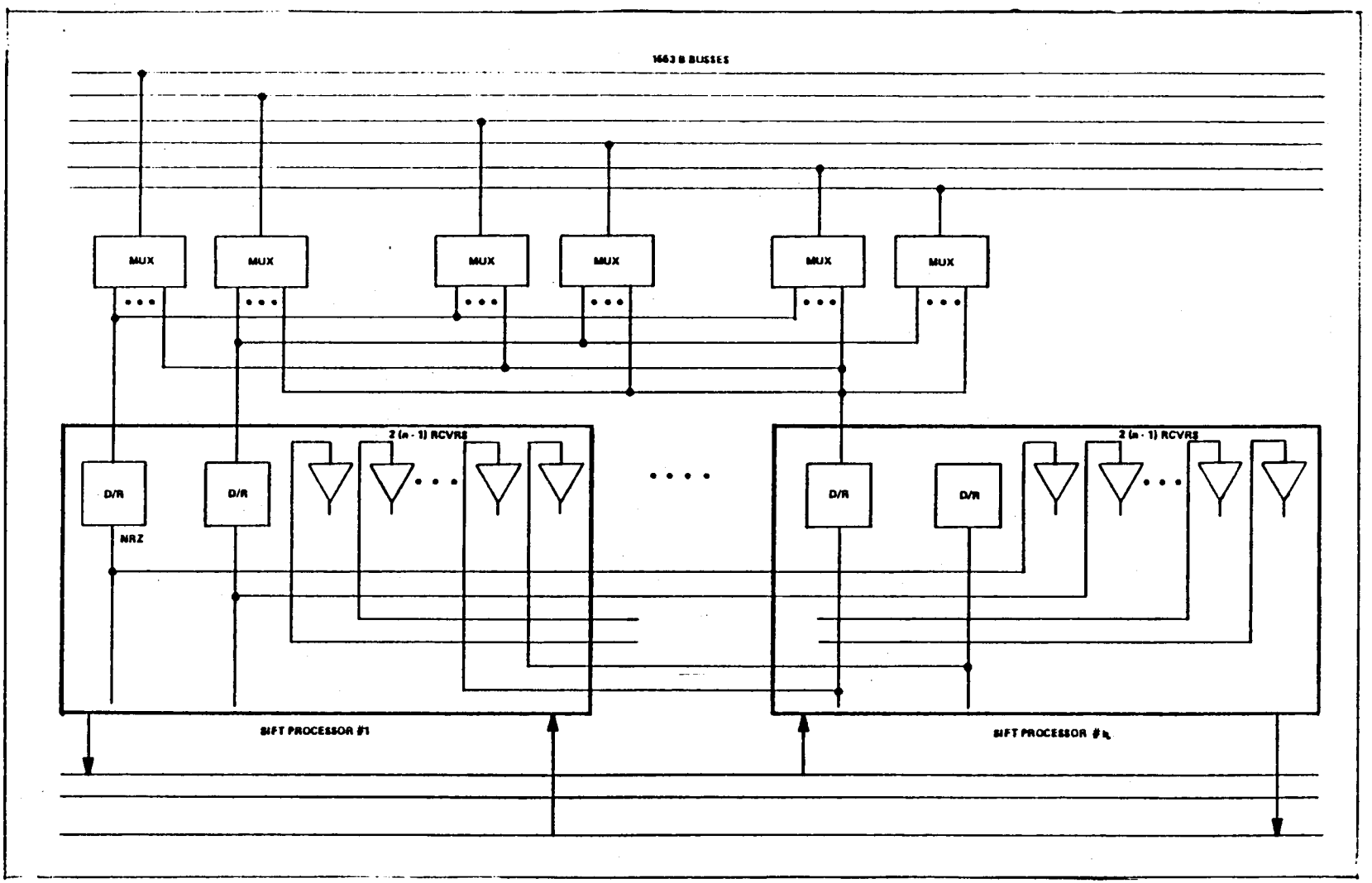


Figure 19 SIFT/1553B Interface Configuration #3

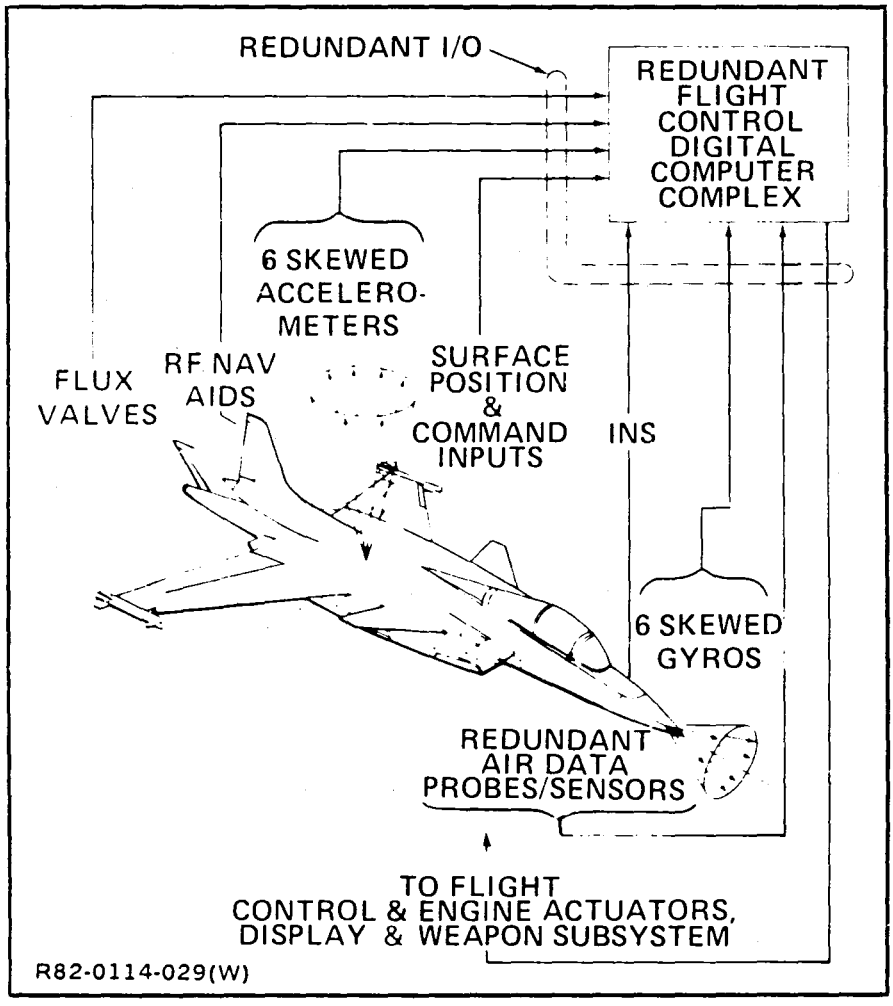


Figure 20 Integrated Sensory Subsystem

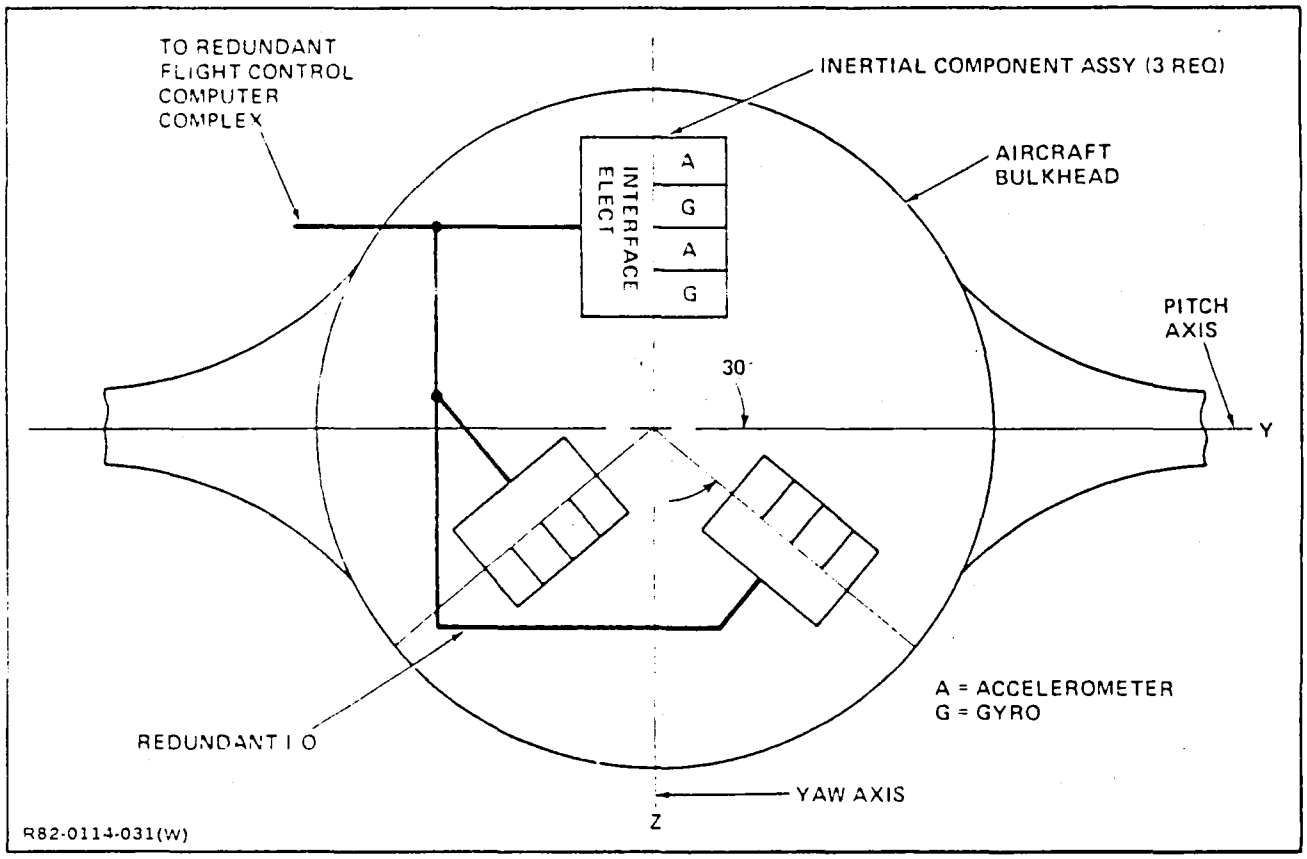


Figure 21 Inertial Subsystem Hardware Configuration

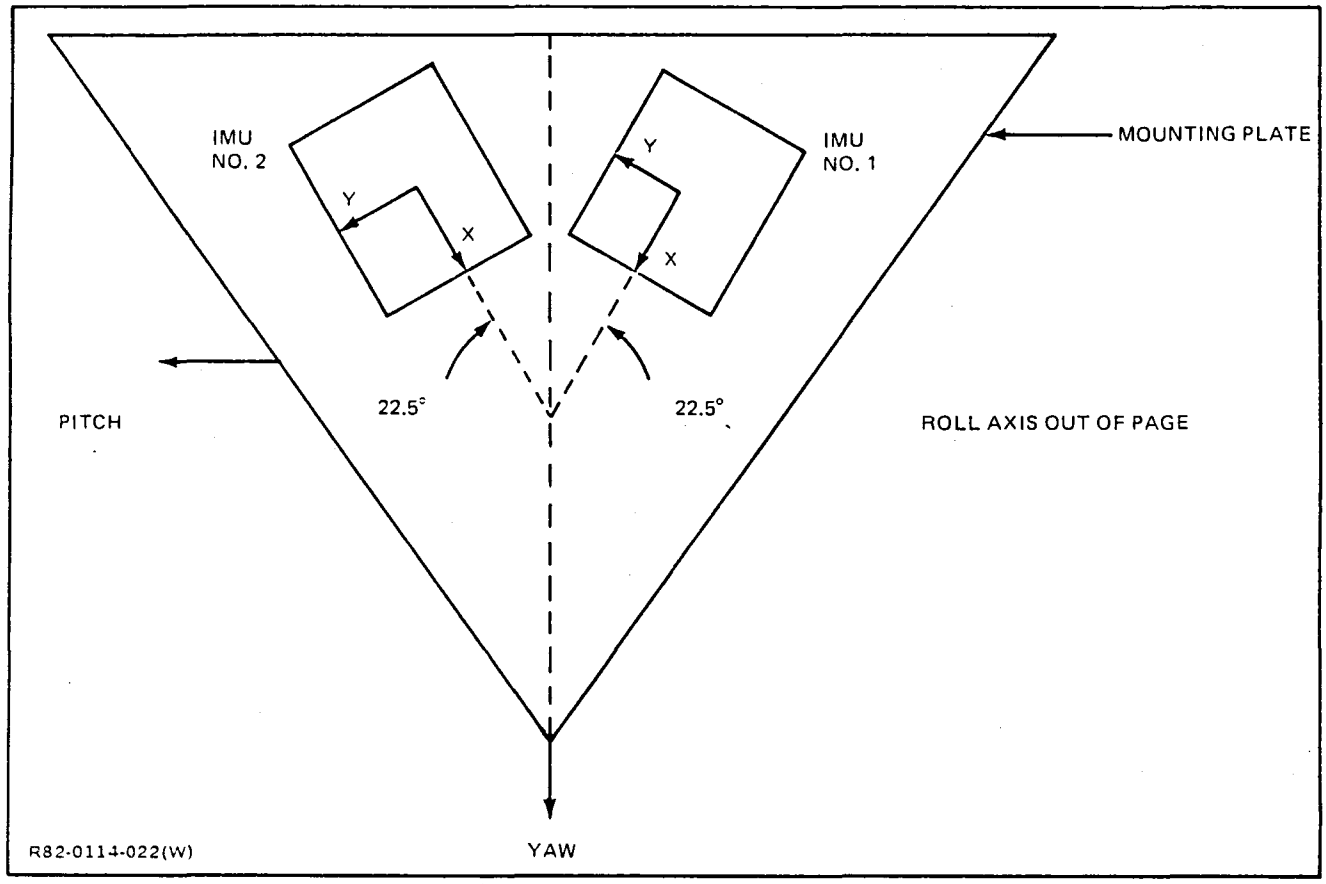


Figure 22 Gyro Configuration

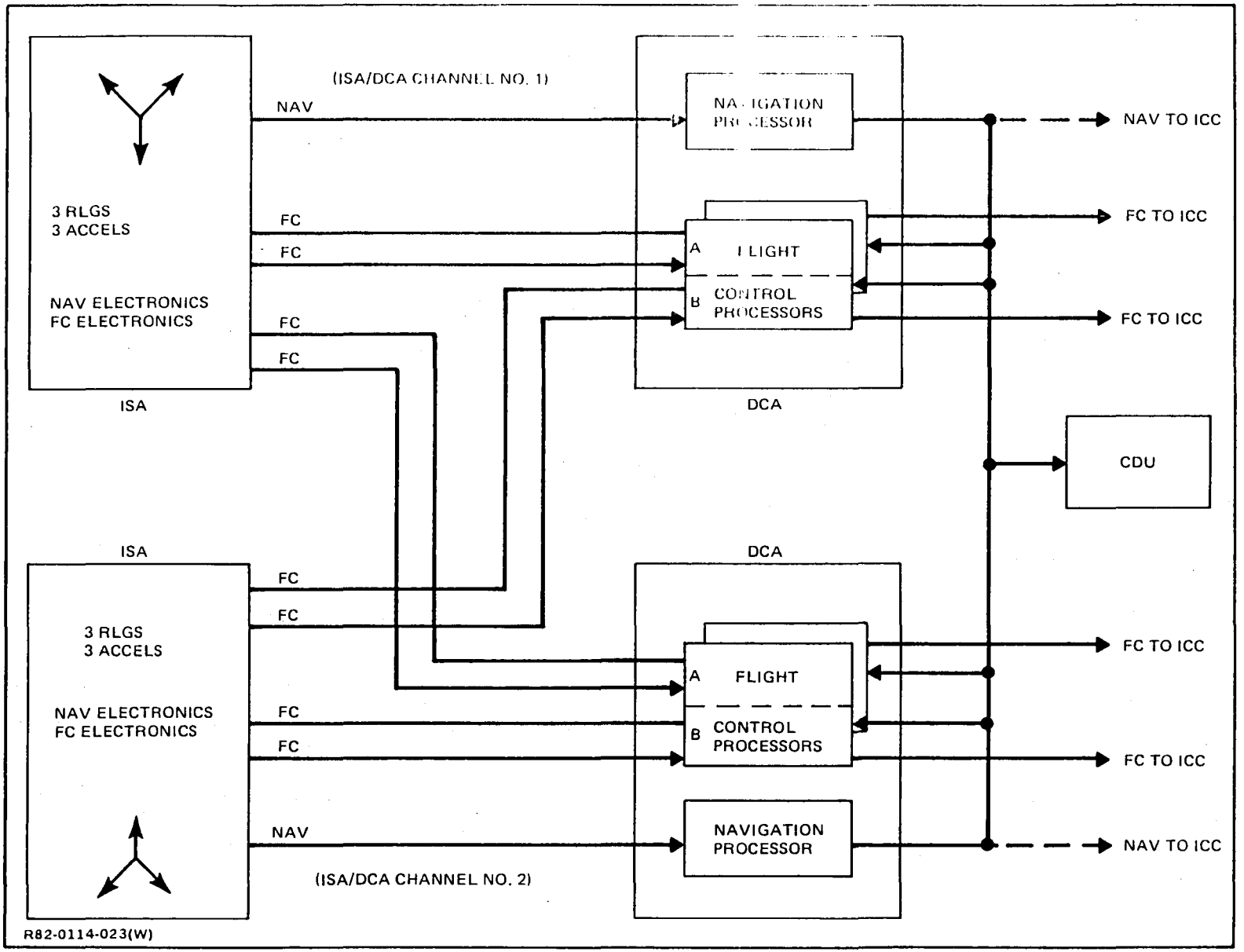


Figure 23 IISA Functional Block Diagram

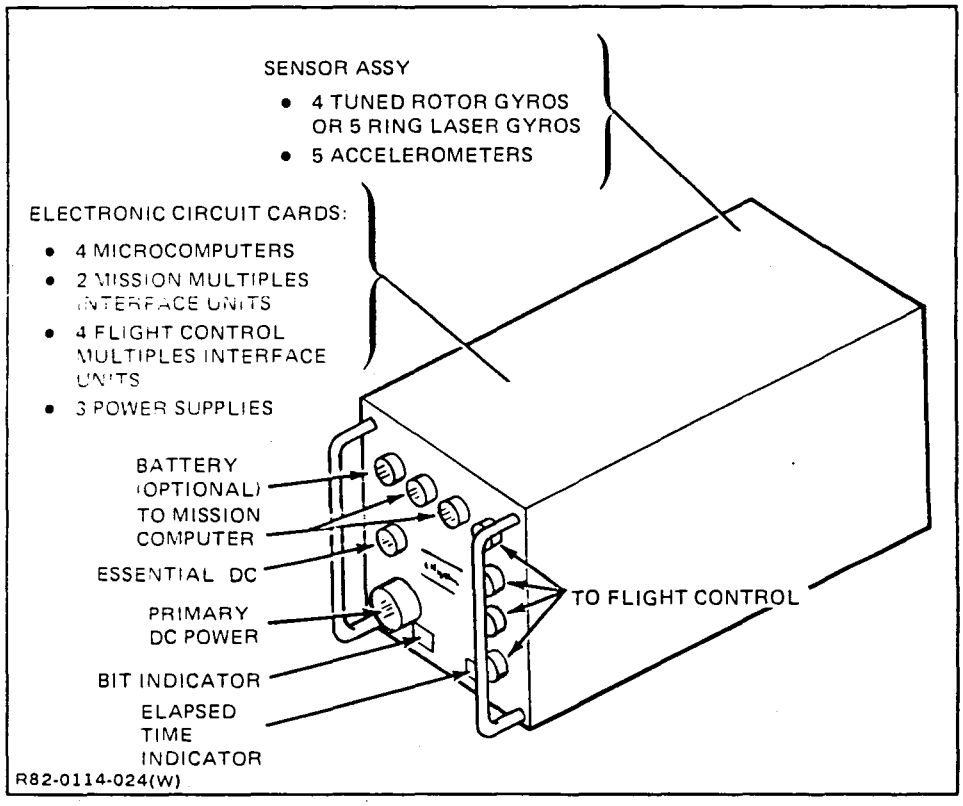


Figure 24 Integrated Sensor Technology, MIRA-Multi-Function Inertial Ref Assy

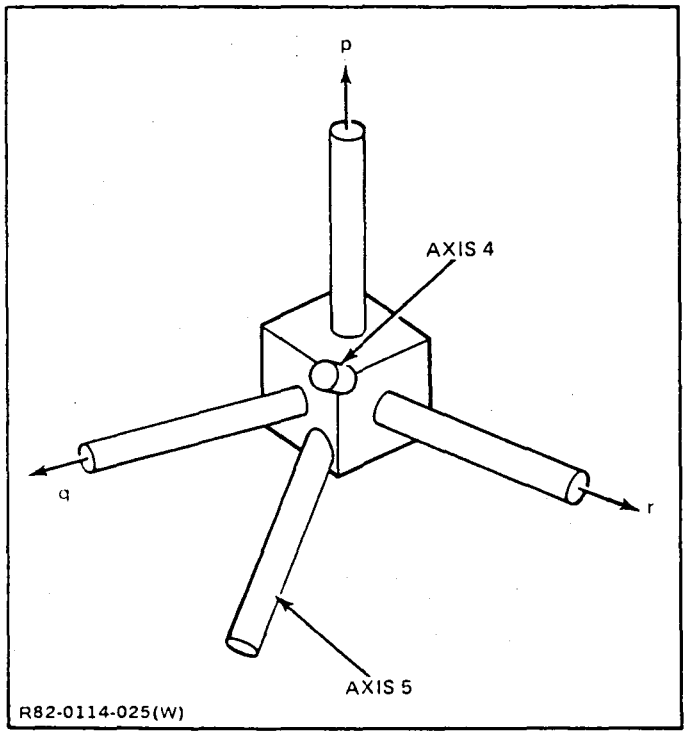
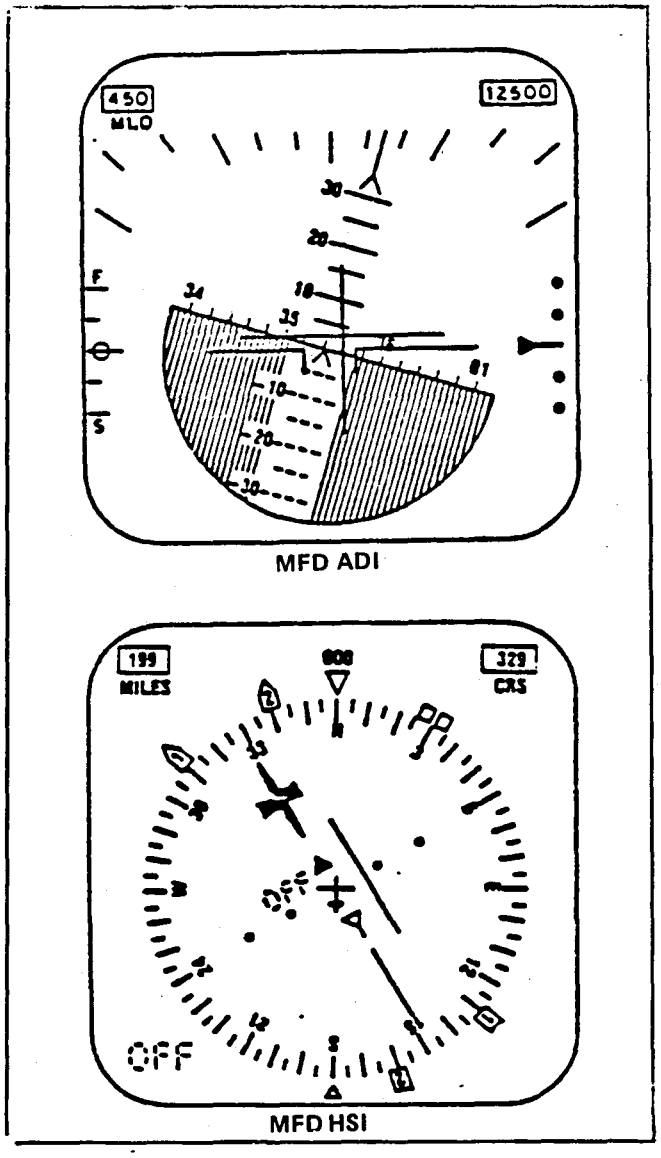


Figure 25 Integrated Sensor Technology,

MIRA-Multi-Function Inertial Ref Assy



MFD ADI

MFD HSI

Figure 26 MFD ADI & HSI Format

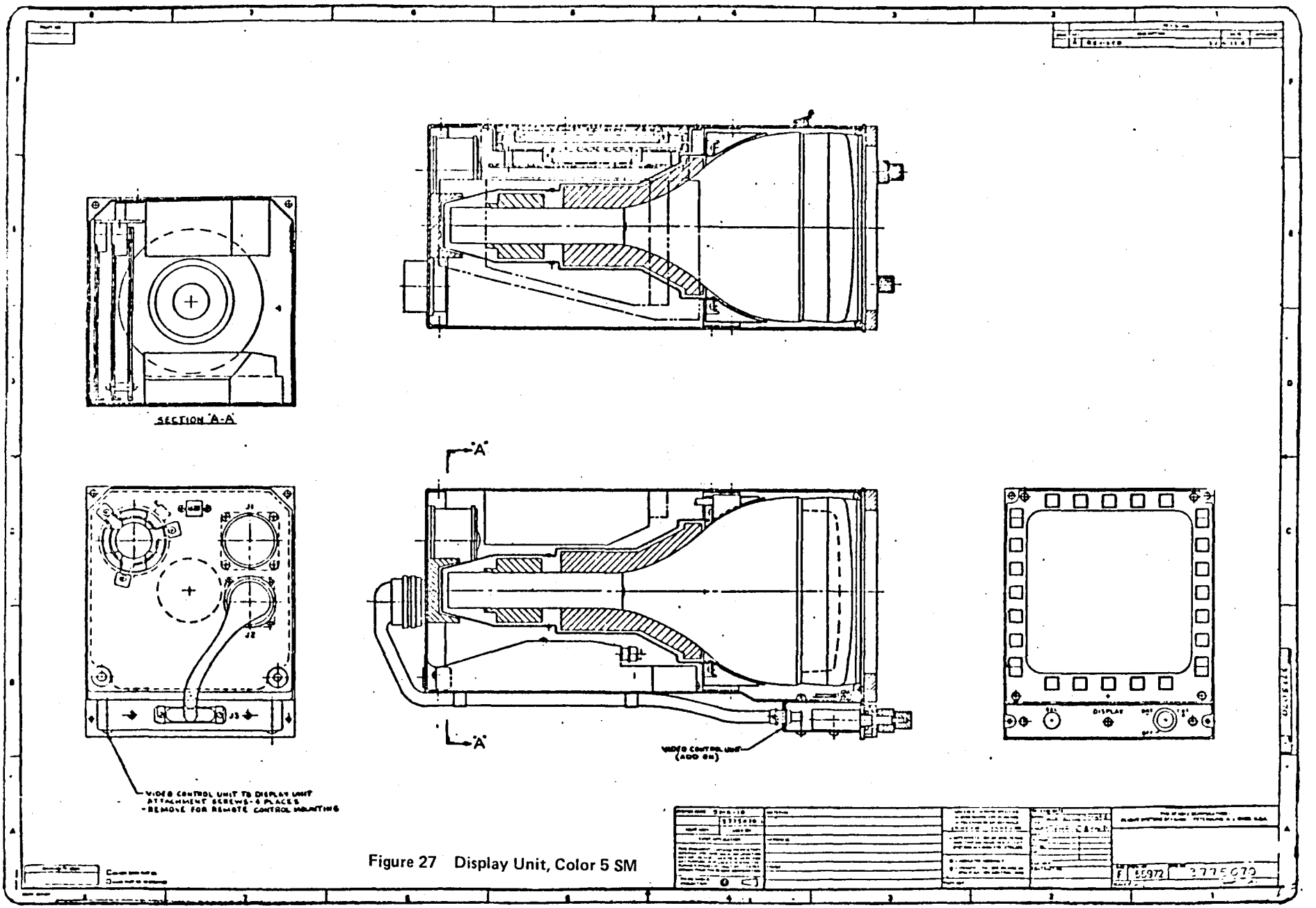


Figure 27 Display Unit, Color 5 SM

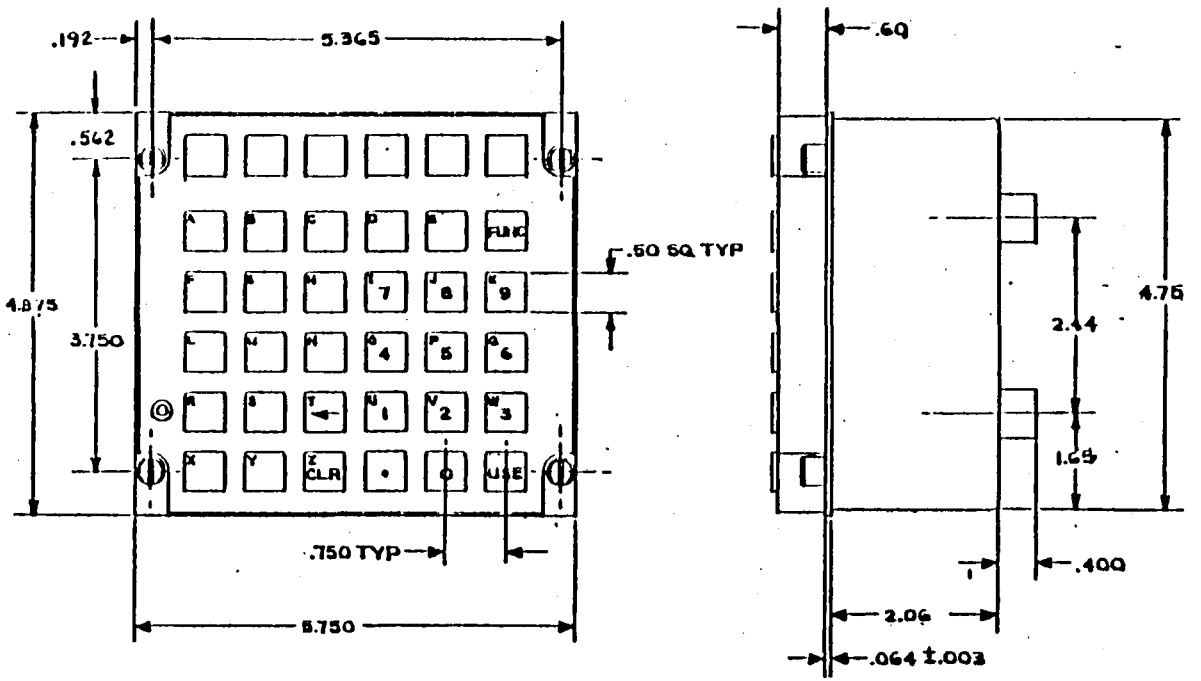


Figure 28 Outline - Keyboard Unit

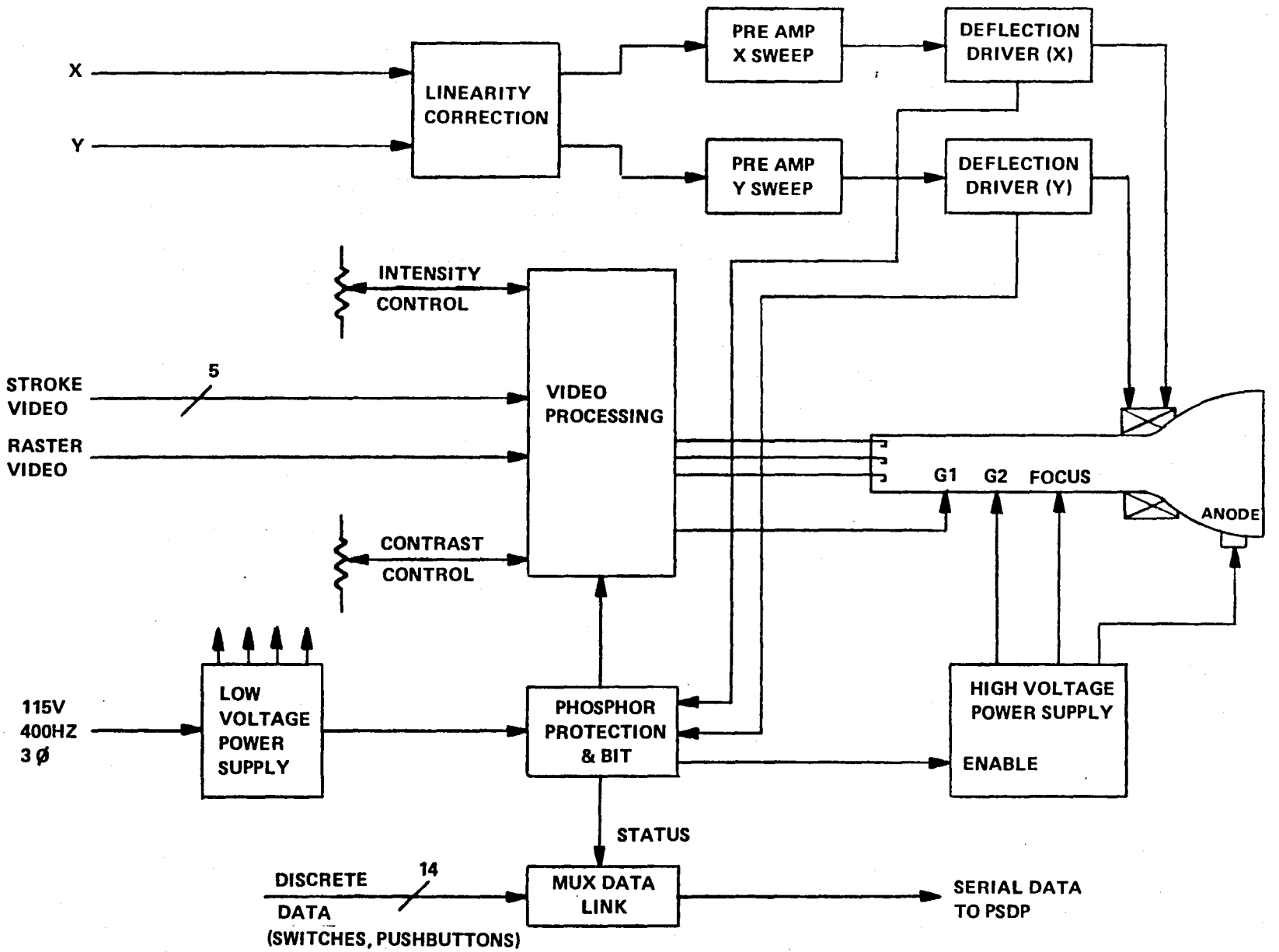


Figure 29 Shadow mask Display Unit Block Diagram

TABLE 1

INTEGRATED SENSOR SYSTEM SUMMARY

PROGRAM	# OF SENSORS	CAPABILITIES	DESIGN STATUS
Baseline configuration (Quad-in-line)	12 Gyros 12 Accelerometers	Fail op, fail op data for flight control, algorithms can be provided depending on the quality of sensors. (1)	N/A
ISS (SDOF config.)	6 SDOF Gyros 6 Accelerometers	Same as baseline	- Skewed gyro redundancy management developed & successfully flight tested. - Skewed gyro and accelerometer redundancy management developed & laboratory demonstrated with flight control sensors. - Lab demonstration of flight control & AHRS capabilities is currently in progress. - Navigation integration with GPS and other NAV systems is under development.
ISS (TDOF Config.)	4 TDOF Gyros 6 Accelerometers	- Same as baseline - The two-box packaging makes this configuration less survivable/ reliable than the three-box configuration for the SDOF gyros.	- Detail system synthesis & lab demonstration is scheduled for calendar year 1981.

TABLE 1

INTEGRATED SENSOR SYSTEM SUMMARY (CONT'D)

PROGRAM	# OF SENSORS	CAPABILITIES	DESIGN STATUS
IISA	6 Gyros (Laser) 6 Accelero-meters	- This system uses inertial quality sensors and thus provides navigation AHRS and flight control - The two-box sensor configuration is less survivable/ reliable than the three-box configuration.	- The system definition phase of this program is complete. - The effort to develop, build and demonstrate hardware is scheduled to begin in calendar year 1981.
MIRA	5 Gyros (Laser) 5 Accelero-meters	- This program also uses inertial quality sensors and will therefore provide navigation, AHRS and flight control system capability. - The single box configuration and the reduced number of sensors used in this program decreases survivability and reliability.	- Exploratory development efforts and lab demonstration phases have been completed. - The follown-on effort, IIRA is scheduled to begin in calendar year 1981. This program will define a system & hardware configuration that will eventually be flight tested.

(1)	GYRO BIAS ERRORS	ACCELEROMETER BIAS ERRORS
Flight Control	60°/Hr	10 mg
AHRS	5°/Hr	2 mg
Navigation	0.01°/Hr	0.1 mg

TABLE 2

INDUSTRY SURVEY: ANALYTIC REDUNDANCY EFFORTS

Draper Labs	Draper labs has been heavily involved with NASA-DRYDEN on the F-8 DFBW aircraft program, specifically in the areas of reliability and redundancy management. The most recent paper by Deckart summarizes F-8 flight test results for an analytic redundancy management system. The conclusions were: 1. Analytic redundancy sensors FDI is sensitive to sensor modeling errors. 2. Elaborate failure mode modeling may be necessary. 3. Sensor bias effects can have significant effects on failure detection rates, but can be accounted for by use of proper techniques. 4. Analytic redundancy is a viable approach.
Boeing	Boeing has performed work for NASA on ARCS-Airborne Advance Reconfigurable Computer System.
General Dynamics	Utilizing the YF-16 with canards, General Dynamics has performed design studies on reversion modes during surface failures. Also performing AFTI F-16 program.
Lockheed	Lockheed is involved in the concept studies for the all-electric airplane and has done some work in redundancy management of this system in transport aircraft.
Honeywell	Honeywell has been involved with the F-8 program and has also performed work in other aircraft design studies (A-7D, F-14A, etc.).

TABLE 2

INDUSTRY SURVEY: ANALYTIC REDUNDANCY EFFORTS (CONT'D)

NASA-Dryden	NASA flight test facility F-8 program, FSW, etc. summary of a F-8 flight experience notes the following: 1. Confirmation of validity AR concept. 2. Need for high quality sensor models for AR. 3. Existing technology can provide low probability of common mode failures in multichannel systems.
Northrop/McDonnell Douglas	F-18 DFBW fighter design; assume AR studies have been performed for this aircraft. Also MFCRS skewed sensor program.
Grumman Aerospace	GAC has performed successful studies in skewed. redundant reconfigurable digital flight control systems (ASSET, ISS, DRDFCS). ASSET was a flight tested article while ISS and DRDFCS have been demonstrated in laboratory utilizing flight hardware. Resulting conclusions are: 1. AR concept is valid. 2. AR can be used to reconfigure flight control system to maintain aircraft operation. 3. AR can be used in air data systems technology.

TABLE 3

SUMMARY OF ANALYTIC REDUNDANCY TECHNIQUES

- Like signal differences for fault detection.
- Unlike signals used to isolate faulty sensor (e.g. derived or estimated signals).
- Signal comparison with derived signals either from other sensors or observers/estimators.
- Blended signals either from direct sensor outputs or combination of sensor, state estimators or observers.
- Modified Sequential Probability Ratio Tests (MSPRT) used in detecting low frequency sensor effects (i.e. bias failures, modeling errors, etc.).
- Elapsed time windows/modified log likelihood tests for transient failure detection.
- Diagnostic Filters - assesses sensor family health. (DF) state estimation technique.
- Super Diagnostic Filter - a DF which can assess a single sensor.
- Interchangeable and non-interchangeable sensors utilizing analytical decision techniques.
- Data reasonableness tests.
- Hypothesis testing - signal whiteness, correlation and mean tests.
- Multiple Hypothesis tests - postulates failure modes and determines likelihood functions. Uses multiple State estimators.
- Parameter identification - use PI to determine sensor parameters for failure indications.

TABLE 3

SUMMARY OF ANALYTIC REDUNDANCY TECHNIQUES (CONT'D)

- Generalized likelihood - use single Diagnostic Filter assuming that failures have particular signatures which are detectable.
- Jump process analysis - failures cause recognizable transient in otherwise stochastic system.

TABLE 4

PROPOSED FLIGHT DEMO GOALS AND METHOD

Analytic Redundancy Management

In presence of detected sensor failure -

- Replace failed sensor with alternate sensor of same type.
- Replace failed sensor with derived signal from similar sensors (skewed technology).
- Replace failed sensor with derived signal from dissimilar sensors (ISS, DRDFCS).
- Reconfigure FCS to perform without signal from failed sensors.

Recommendations

For a flight demo in 1985 -

- Generalized Likelihood Ratio Method
  - single State estimator which detects failures by their signature.
  - utilization of extensive experience in State estimator design and extend to formulation of likelihood functions.
- Reconfiguration techniques similar to ISS, DRDFCS.

TABLE 5

ACTUATION SYSTEMS SUMMARY

CONFIGURATION/PROGRAM	BENEFITS/FEATURES/ADVANTAGES AND DISADVANTAGES	STATUS & FORECAST FOR FUTURE APPLICATION
ELECTROMECHANICAL ACTUATION SYSTEMS: • Boeing Commercial Airplane Co. • Boeing Military Aircraft Co. • Lockheed California Co. • Grumman Aerospace Corp. • Honeywell, Clearwater, Fl. • Airesearch, Torrance, Ca. • AFWAL; NADC; NASA Headquarters; NASA JSC; NASA DFRC	BENEFITS/FEATURES/ADVANTAGES • Increased Energy Efficiency • Reduced Life Cycle Cost • Reduced Weight • Significantly Less Fuel Consumption • Improved Dispatch Reliability or Operational Readiness DISADVANTAGES • Probable Higher Initial Cost • High Cost, Moderate Risk Development Program Required	• Single axis flight test program from 1982 thru 1984 - roll & yaw axes • Pitch axis & 3 axis flight test programs 1984 thru 1988. • Viable candidate for consideration for a new aircraft design in: - 1988 thru 1992 for a small to medium size, subsonic aircraft - up to 150 passenger transport, AEW, ASW or similar aircraft. - 1992 - 2010 for large transports or fighter/attack aircraft.

TABLE 5

ACTUATION SYSTEMS SUMMARY (CONT'D)

CONFIGURATION/PROGRAM	BENEFITS/FEATURES/ADVANTAGES AND DISADVANTAGES	STATUS & FORECAST FOR FUTURE APPLICATION
DIRECT DRIVE VALVES		
• North American - Columbus Division • McDonnell Douglas • Most Hydraulic Actuator Suppliers - MOOG; National Water Lift; Bendix Electrodynamics; Bertea; etc. • NADC; AFWAL	BENEFITS/ADVANTAGES • Increased Reliability • Reduced Cost, Complexity, Weight • Reduced Maintenance • Eliminates EHV Null Flow Losses • Simplifies Interface with Hydraulic Systems & Redundant FBW System DISADVANTAGES • Increased Electrical Power Levels Req'd • Chip Shear Forces tend to be Low • Reliability Base for Jam Free Motor & Valve Combination • EMI Generation	• First generation flight test programs 1981 thru 1982. • Second generation flight test of production type hardware 1982 - 1984 • Integrated studies & test programs - 1983 to 1986. • Production application decision point - 1985 to 1987.

TABLE 5

ACTUATION SYSTEMS SUMMARY (CONT'D)

CONFIGURATION/PROGRAM	BENEFITS/FEATURES/ADVANTAGES AND DISADVANTAGES	STATUS & FORECAST FOR FUTURE APPLICATION
INTEGRATED ACTUATOR PACKAGES (IAP):		
• Boeing Military Aircraft Co. • North American Div. of Rockwell International • Sperry Vickers • Bendix Electrodynamics • AFWAL	BENEFITS/ADVANTAGES • 80% to 90% Efficient vs. 50% to 60% for Conventional Approach • Controlled Variable is usually Pump Displacement - is a Power Demand Device • Negligible Velocity Variation with Load • Approximately 70% Power Savings • Up to 400% Reliability Increase • Up to 55% Weight Savings • As much as 2x Survivability Enhancement DISADVANTAGES • More Complex & Probably More Costly • Thermal Problem in Some Applications	• Successfully used on VC-10 transport. • New generation hardware in early development stages. • Flight tests planned in 1982 through 1984. • Transports & other subsonic aircraft would be candidates in 1983 - 1986. • Questionable for application to flighter/attack aircraft due to heat problem.

TABLE 5

ACTUATION SYSTEMS SUMMARY (CONT'D)

CONFIGURATION/PROGRAM	BENEFITS/FEATURES/ADVANTAGES AND DISADVANTAGES	STATUS & FORECAST FOR FUTURE APPLICATION
LIGHT WEIGHT/HIGH PRESSURE HYDRAULIC SYSTEMS - U.S. NAVY PROGRAM: • North American, Columbus Division of Rockwell International • Vought • Grumman • Numerous Equipment Suppliers • NAVAIR; NADC	BENEFITS/ADVANTAGES • 25% to 30% Weight Savings Possible • Significant Reduction in Volume • Increased Survivability • Improved Reliability & Maintenance DISADVANTAGES/PROBLEM AREAS • Actuator Stiffness • Development Risk • Reliability • Standardization & Safety Considerations • All New Ground Support Equipment Req'd • Heat Rejection	• Preliminary flight test program completed. • More extended but limited flight test program scheduled in 1981 - 1983. • Possible production decision point in 1983 - 1985.

TABLE 5

ACTUATION SYSTEMS SUMMARY (CONT'D)

CONFIGURATION/PROGRAM	BENEFITS/FEATURES/ADVANTAGES AND DISADVANTAGES	STATUS & FORECAST FOR FUTURE APPLICATION
ROTARY ACTUATORS:		
• Electromechanical - Airesearch, Torrance, Ca. - Grumman - AFWAL - NADC • Electrohydraulic - Hydraulic Units, Inc. - Bendix Electro-dynamics - McDonnell Douglas	BENEFITS/ADVANTAGES • Ideal for Thin Wing & Restricted Space Envelope Applications • Usually Designed as Hinge Line Units DISADVANTAGES • Generally More Costly • Long Development Time Req'd • Small to Moderate Risk Involved	• Electrohydraulic used on rudder of F-15. • Electromechanical type mechanization used on flap/slat drives of F-16 and/or F-18. • Technology available now for some applications

TABLE 6

DISPLAY UNIT CHARACTERISTICS

TYPE NO:	3775073-1
INPUT POWER:	115 VAC, 3 Phase, 400 HZ at 100W, 28 VDC at .07A
WEIGHT:	12.5 Lbs.
CRT:	5 x 5 shadow mask
	Vertical - 5.0 inches
	Horizontal - 5.0 inches
	Diagonal - 6.7 inches
	Neutral density filter
OPERATING MODE:	Stroke
	Raster (525 line std.)
	Raster with stroke overlay
INTERFACE SIGNALS:	Horizontal Deflection
	Vertical Deflection
	Raster Red Analog Video
	Raster Green Analog Video
	Raster Blue Analog Video
	Stroke Red Logic
	Stroke Green Logic
	Stroke Blue Logic
	Blanking Logic
	Raster/Stroke Logic (Source/Mode Switching)

TABLE 6

DISPLAY UNIT CHARACTERISTICS (CONT'D)

PHYSICAL DIMENSIONS:		
	Bezel:	Height - 6.75 inches
		Width - 6.50 inches
	Display Unit:	Height - 6.63 inches
		Width - 6.38 inches
		Length (excluding connector) - 13.58 inches
	Control Unit:	Height - 1.1 inches
		Width - 6.5 inches
		Length - 2.4 inches
RELIABILITY (MTBF)		6062 HOURS

5.0 FORMULATION AND DESCRIPTION OF ADVANCED ARCHITECTURE CONCEPTS

5.1 Introduction

The last decade has witnessed the accelerating use of digital technology in aircraft systems. Low cost, greater reliability, and enhanced performance coupled with the emergence of active controls and energy efficient aircraft were the major factors influencing this trend. One objective of this study is to assess recent developments and new directions in digital technology which show promise in supporting the goals of full-time, full-authority and highly reliable control systems.

As control systems evolved through several generations of aircraft, it was recognized that full-authority controls could provide significant benefits in performance and economy. However, such systems are necessarily flight critical since a malfunction could result in loss of the aircraft. As a consequence, survivability has become the paramount consideration in their employment. For purposes of this study a "highly reliable system" is one which has a survivability rate no less than 10 -10/hour of flight; this is several orders of magnitude beyond the goal of current FBW control systems, (Typically, 10 -7/hour). Failure rates of digital components are not expected to improve sufficiently to meet either of these goals without employing some degree of fault-tolerant capability. Thus, an advanced architecture will consist of a computing complex that must survive its own failures, detect and isolate failures throughout the system and manage the reallocation of surviving resources. The responsibility for containing faults and maintaining access to surviving resources wil fall heavily on networks which carry data signals to the dispersed elements of the system. Thus, we have the two essential elements of the highly reliable system:

- A communications network capable of supporting the requirements of data transmission, failure management and reliability
- A fault-tolerant computing complex

It is our considered opinion that, with few exceptions, the technology base necessary to support the goals of an advanced control system exists. It is only necessary to apply that technology in new and innovative directions.

5.2 Conventional Architectures

Some of the deficiencies of conventional architecture have already been alluded to in Section 4.5. These and others are briefly summarized:

Deficiencies of the Conventional Architectures

- Dedicated, hardwired interfaces
- Unique signal conversion hardware
- Large variety of signal formats
- Effective redundancy requires hardware duplication (e.g. for cross-strapping)
- Little or no sharing of resources
- Poor growth capability

We can roughly describe the conventional flight control system as consisting of dedicated sensors, computers and actuators with dedicated and specialized communication links between the sensors and computers, between the computers and actuators and between the computers, themselves. Sensors are monitored by the computers which employ relatively complicated voting and monitoring algorithms for this purpose. Actuators are monitored by internal mechanical or hydraulic logic and/or by the computers. And the computers always monitor each other. The result of this is:

- A large proportion of real time is used to input, output and monitor system variables.
- Reconfiguration is reduced to the simple strategy of disengaging a failed element.
- Expansion is difficult and usually requires a significant system redesign.
- Spare subsystems are not easy to incorporate, even if available.

The impact of these properties will be assessed in Section 6.0.

5.3 Advanced Architecture

Apart from the threshold qualifications of economy and reliability, the key factor in the selection of an advanced architecture is its ability to provide a communications structure that is flexible and allows the designer maximum scope in implementing a control concept. Thus, for example, the structure should accommodate a centralized or distributed

system; sequential or parallel processing; hierarchial bus structure; centralized or distributed monitoring; synchronous or asychronous control; voting and masking failures, etc. In addition, it is desirable that the structure consist of familiar and accepted technologies.

The advanced architecture consists of the following elements:

1. a bus network;

2. an ultrareliable multiprocessor bus controller;

3. a set of sensors and sensor interface processors;

4. a set of actuators and actuator interface processors;

5. a set of application processors;

All of these elements would be connected to a single, local network consisting of dual, 1553B busses. If a single local network did not have sufficient bandwidth it would be necessary to employ a second network. An example of the structure is shown in Figure 30 for the subsystems of a typical flight control system. The levels of redundancy shown in the diagram are for illustrative purposes, only, and do not necessarily imply firm requirements.

DESCRIPTION OF SYSTEM ELEMENTS

1. Bus Network

   The bus network consists of local networks of dual, 1553B busses, as described in Section 4.5. The principal issues associated with the bus network are:

   - available bandwidth,
   - quantity of remote terminals accommodated,
   - vulnerability to single point failure,
   - transmission errors

Bus loading estimates are given in Appendix A. There it is shown that bus utilization for a typical flight control system for a commercial transport is 86%, assuming a single bus at a 1 MHZ transmission rate.

Although this estimate is conservative, it does indicate that at least two, independent busses would be required. A modest increase in bus bandwidth, e.g. to 4 MHZ, can be expected in the near future. A 4 MHZ bandwidth will certainly be sufficient for flight controls for current aircraft.

The terminal limitations (e.g. 31 terminals, maximum) is more difficult to overcome since any expansion requires a modification of the 1553B protocol. The restriction to 31 terminal limits the degree of distributed processing that the network can accommodte.

The vulnerability of 1553B to single point failures can be overcome by providing dual or triplicated busses, only one of which is active at any given time. Preliminary analysis of bus and terminal failure modes indicates that a dual bus would provide the necessary survivability.

There are two kinds of transmission errors associated with 1553B: detected and undetected bit errors. The detected errors are characterized by the word error rate (WER) which is specified in (Ref (10) to be

WER = 10(-7) errors/word.

Since the bus protocol allows for an immediate retransmission of the faulty data, the detected errors have a negligible effect on system operation.

The undetected errors are characterized by the bit error rate (BER) which is specified in Ref (10) to be

BER = 10(-12)/bit,

which is equivalent to 3600 x 10 (-)6 errors per hour at a 1 MHZ transmission rate. The intended failure detection strategy employs persistence counting before a subsystem element is permanently disengaged,, e.g. it is disengaged only if the error persists for a prescribed number of frames. As a consequence, if voting is employed by subsystems using this data then the fault can be masked during the persistence counting. This assumes that the persistence count is not so long and the probability of a second, independent failure so high that it would defeat the voter. This is usually the case. Thus, under normal conditions, undetected bit errors have a negligible effect on system operation.

2) An Ultrareliable Bus Controller

The advantages of an ultrareliable bus controller are:

- Redundant, critical components can be connected to a single local network.
- The bus controller can be used to monitor all system variables and monitor system status.
- The bus controller can function as the system reconfiguration manager.
- The bus controller can supply an accurate clock to the system.

All of these functions are critical and require, for their implementation, an ultrareliable bus controller, i.e. 10 (-10)/hour probability of functional failure.

It is intended to use a SIFT-type multiprocessor to perform the functions of bus control for the entire system. The interface between the bus controller and the local network has already been described in Section 4.5. As indicated in that section, a redundant set of processors is assigned control of a local network but only one processor actually controls the network at any given time. When the controlling processor fails, it is disengaged from the local network by an independent switching network. The switching logic is obtained by majority-voting failure discretes supplied by the SIFT processors. The functional schematic of this interface is shown in Figure 31, two possible implementations are shown in Figure 32, one of which employs mechanical and the other, solid state switching. Since a processor remains in control of a local network until it fails, the duty cycle of a switch will be small and the switching transient will have a negligible effect on systems operation.

We note that the proposed bus interface hardware can be used to implement a system of independent, redundant busses. However, the approach taken in this study is to transmit redundant data over a single local network rather than over several such networks.

The reliability of the proposed interface has yet to be determined but it is expected to be at least 10 (-10)/hour. The principal failure modes are:

- a normally open switch closes;
- a switch remains open;

- an isolation amplifier shorts;
- the address logic fails.

Normally, each processor sets its isolation amplifier to its high impedance state when it is not in active control of a local network. As a consequence, a normally open switch closure will have no effect even if the associated processor eventually takes control of the bus (the switches are assumed to be independent).

A switch that cannot close will result in the inabiity of the associated processor to control the bus. This failure will be detected by the bus control monitors when the affected processor eventually assumes control of the bus.

A failed isolation amplifier can have several effects, depending upon the nature of the fault. In the worst case it will result in disengagement of the associated processor when it assumes active control of a bus.

A fault in the address logic will connect an unassigned processor to the bus and disengage the assigned processor. The unassigned processor's isolation amplifier will be in the high impedance state and, consequently, the fault will appear to be a failure of the bus. The assigned processor will then revert to a standby bus for subsequent communications.

The proposed interface circuitry is clearly sufficient to prevent single failures from disabling a local network. The potential risk is combinations of faults that can do so, for example, a normally open switch closure followed by a processor failure which activates the isolation amplifier associated with the failed switch. If the faulty processor is malicious it could direct all remote terminals to disengage themselves from the standby busses, thus, effectively disabling the entire local network. While such failures are undoubtedly highly improbable, a detailed failure analysis is required before any proposed arrangement can be considered firm.

Several interface configurations for bus monitoring have been proposed in Section 4.5. The recommended configuration is shown in Figure 17. In this arrangement a processor can listen to any local network but only one network at any given time. Normally, at least three processors will listen to the traffic on a local network for the purpose of:

- monitoring the bus controller,
- monitoring redundant system variables

Monitoring The Bus Controller

Since each processor listens directly to the bus transactions, it can monitor the bus controller independently of the other processors. Thus, monitoring can be made effective and timely. Because the bus controller is passive, i.e it does not transmit data, a faulty bus controller can, at worst, inhibit bus transactions until it is disengaged. Thus, the time to detect and diagnose a faulty bus controller is determined by the effect of this hiatus on system performance. While this effect will depend upon the system characteristics it is reasonable to assume that a hiatus equal to the smallest iteration interval of a critical subsystem is acceptable. In the case of a flight control system for a current commercial aircraft, this could be as large as 50 miliseconds. If we assume an average of 10 words/message in a typical RT to RT transaction, then a single message requires 306 microseconds for completion (see Appendix A for bus transaction times) or, approximately, 3 messages per milisecond or 150 messages per primary cycle. This is ample data on which to base a detection strategy.

Monitoring Redundant Variables

It is intended that all redundant variables transmitted on a local network will be monitored by the bus controller. This relieves the users of a very considerable real time burden and makes the bus controller responsible for the integrity of data transmitted on the bus.

A preliminary analysis indicates that, even under the most pessimistic conditions, the bus controller has sufficient time to perform the monitoring task. To assess this capability we assume that a message of 32 words is sent in triplicate via an RT-to-RT transmission at the maximum rate of 1 MHZ. The time to transmit the three messages is 2238 microseconds (see Appendix A). Thus, the time to transmit a single variable, in triplicate, is

$$2238/32 = 69.94 \text{ microseconds}$$

Based on a comparison-monitoring algorithm developed by Bendix and executed on a Bendix BDX-930 processor, the time to perform a 3-way comparison is 48 microseconds. Thus, even in the most improbable scenario (i.e. 32, triple redundant variables with a refresh time of 2238 microseconds) there is sufficient time to perform the monitoring task.

In practice, it is proposed to monitor each redundant variable during its minor cycle transmission, i.e. the minimum refresh time. As a consequence, the variable could be in error during this time and not be identified as such. Subsystems using this data would have to either tolerate the error or incorporate input voting to mask the error. When an error is attributed to a source the bus controller will:

- inform all users of the error and/or,
- supply an alternate variable and
- continue to monitor the variable for persistence.

Bus Protocol

Bus protocol will consist primarily of RT-to-RT and broadcast transmissions. Although the bus protocol can accommodate asynchronous transmission, it is expected that, in the majority of cases, the bus controller will direct transmission in a fixed, periodic sequence, the update rate of each variable being determined by the performance requirements of the users, i.e. effects of transport delays.

Redundant data can be transmitted in several ways:

1. Each redundant variable is associated with a different user and is transmitted to that user via the RT-to-RT mode. The other users, meanwhile, input the variable as in the broadcast mode. The assigned user is responsible for return of the "STATUS" word.

2. All redundant variables are transmitted in the broadcast mode. The bus controller assumes responsibility for the integrity of the data.

The former protocol is preferred even through it requires a modification of terminal decoding and response procedures. This approach a) insures that at least one user receives the data correctly and b) provides redundant data for input voting without the penalty of redundant transmissions.

3) Sensors and Sensor Interface Processors

Sensors are grouped into dissimilar sets with each set serviced by a sensor interface processor. Each processor would:

- input a sensor,
- provide the appropriate signal conditioning,
- format and transmit the encoded signal to the local network. In a totally distributed system each processor would be dedicated to a single sensor. Signal conditioning would take cognizance of the users' requirements and the dynamics of the digitizing process would be documented and made available to all users.

A typical triply redundant sensor interface is shown in Figure 33.

As indicated previously, the proposed architecture does not preclude private busses between subsystems. Although it is intended that the bus controller will monitor redundant variables it is recognized that in some instances this may not be practical, i.e. in the case of skewed sensors. In such cases the interface processor could perform this function, using a dedicated bus for interprocessor communications.

One of the advantage of the sensor arrangement is that spare sensors can be incorporated by simply connecting their associated processors to the local network. In this way any number of spares can be accommodated with a negligible impact on the system architecture.

4) Actuators and Actuator Interface Processors

The proposed architecture imposes no constraints on the actuation system other than that it must provide sufficient survivability and be able to incorporate spare units as may be required by the maintenance strategy. Indeed, it is intended that the actuator configuration be transparent to other subsystems. It is only required to provide an interface between the actuator and the local network. One possible arrangement is shown in Figure 34 for a single primary actuator. The secondary actuators are quadruplex and mechanically summed and each is serviced by an actuator interface processor. An interface processor could service several different actuators, depending upon the degree of dispersal desired. Each actuator processor would, as a minimum,

- input actuator commands from the local network,
- provide the appropriate signal conditioning for the selected command,
- transmit this command to the secondary actuator.

Actuator commands are monitored by the bus controller. As described previously, each redundant command is associated with a dedicated interface processor and is sent to that processor via an RT-to-RT transmission; the other processors receive the same data as in the broadcast mode. All processors would perform input voting to mask a command error.

Monitoring the actuators and actuator interface processors is the responsibility of the respective subsystem. It is expected that monitoring techniques will be similar to those employed in conventional systems.

5) Application Processing

The application processors perform tne control computations for the system. As stated previously and emphasized repeatedly, the bus structure provides the maximum flexibility for implementing a control concept and this applies particularly to the application processors. This flexibility is illustrated in the following paragraphs.

SIFT Multiprocessor Systems

The proposed architecture can accommodate a SIFT-type system by simply connecting the individual processors and standbys to the local network. The processors could perform the same control computations, voting, and monitoring as formerly, using the dedicated broadcast busses for interprocessor communication. The only difference is that, in the proposed architecture, there exists a "smart", independent and ultrareliable bus controller to monitor inputs and outputs to the local network. Now, when an individual processor fails, the failure status is communicated to the bus controller which then takes the appropriate reconfiguration action. This consists primarily of substituting the outputs of another processor for those of the faulted processor. It is no longer necessary to have user subsystems monitor SIFT outputs and failure status.

The proposed architecture and the expanded role of the bus controller are entirely compatible with the SIFT concept. A typical applications processor interface is shown in Figure 35.

Distributed System

SIFT performs all of the control computations for the system and is directed in this activity by a Central Executive program that is replicated on each SIFT bus controller. While SIFT is effectively a centralized system its component processors could be physically dispersed along the local network. In a distributed system, on the other hand, the control tasks

are partitioned among sets of application processors, each at a level of redundancy commensurate with the criticality of the task. These subsystems perform reduced tasks and operate more or less independently of each other. The vulnerability of the distributed system to single faults is less than in the larger computer complex since there are fewer "eggs in one basket". Moreover, the complexity of applications software is reduced since the control functions are partitioned over small, independent modules instead of being time shared in a single centralized computer. The proposed separation of sensor and actuator interface processors is a further step in the direction of distributed processing, and distributed software.

The physical arrangement of distributed application processors would be identical to that of Figure 35 except that there would be many such subsystems connected to the local network.

Monitoring the application processors can be performed by the bus controller or by the subsystem, itself. As with other subsystems the bus controller monitors all outputs to the local network. When an error is detected, the bus controller, thereafter, ignores the errant processor's outputs and delegates an alternate or standby unit to perform the same function and arranges a transfer of initializing data from an on-line to the standby processor. Another approach is to allow each subsystem to monitor itself. When a fault is detected the subsystem communicates the fault status to the bus controller for reconfiguration action.

Another approach to control of either the centralized or distributed system is parallel processing. This approach is described in Section 6.

5.4 PHYSICAL LOCATION OF ELECTRONICS

A trade-off of alternate locations of flight control and avionics electronic equipment for a transport aircraft was conducted in (Ref (7) from the point of view of a) damage tolerance, b) wire length/cost savings, c) environmental conditions and d) maintainability. The configurations considered were:

LOCATION ALTERNATIVES CONSIDERED

One Bay	One primary electronics area located near nose under cockpit.
Two Bay	Primary electronics separated as much as possible into two areas preferably separated by a bulkdead to increase damage tolerance.

Three Bay	Same general location as two bay with reduced fault tolerance within each bay.
Six Bay	Electronics located within pressurized fuselage as close as practical to the associated equipment/actuators/sensors.
Nine Bay	Same general locations as six bay with reduced fault tolerance within each bay.
Multi-location	Selected electronics are located outside pressurized fuselage in order to be close to equipment being serviced.
Embedded	Electronics either embedded within equipment being serviced or in very close proximity. This is the fully dispersed arrangement.

Although the assumptions on which the trade-offs were based do not exactly apply to the proposed architecture (principally in the structure of the bus network) the conclusions are sufficiently general to be applicable to a variety of architectures and are, therefore, worth summarizing here.

SUMMARY OF CONCLUSIONS

One Bay

- Excellent maintainability and environment
- Intrabay communications short and protected
- Excessive amount of dedicated wire required for remote equipment
- Damage tolerance may be too low to support fully flight crucial functions

Two Bay

- Essentially the same maintainability, environment, and wiring as one bay
- Some interbay communications required
- Damage tolerance increased to allow full flight crucial functions

Three Bay

- Essentially the same maintainability, environment, wiring, and damage tolerance as two bay
- Fault tolerance within each bay can be reduced
- Allows straightforward interface with triplex actuators

Six Bay

- Environment essentially the same as the one and two bay with maintenance only slightly less convenient
- Total wire required significantly reduced
- Damage tolerance increased
- Intrabay communications more complex

Nine Bay

- Expands six bay configuration to reduce the fault tolerance requirements of the three bay

Multi-location

- Wire lengths again significantly reduced
- All locations no longer have to provide high levels of internal redundancy
- Environment and maintainability for some locations considerable degraded
- Interlocation communications becomes more critical

Embedded

- Wire lenghts reduced to minimum
- Supports high degree of fault and damage tolerance
- Maintenance and environment extremely bad for some equipment
- Reliability for electronics must be very high to avoid significantly reducing the reliability of the equipment in which it is embedded (not currently possible in some cases)

The conclusions indicate that, from the standpoint of damage tolerance and reduced wire length, distributed deployment (i.e. multi-location and embedded) is preferred. The disadvantages of degraded environment and poor maintainability make distributed deployment risky, at the present time. The 3-bay and 6-bay arrangements appear to be reasonable compromises provided that they can be made sufficiently tolerant to damage. A 6-bay configuration employing a dual bus is shown in Figure 36.

Relative to damage tolerance a deployment strategy for the advanced architecture will be strongly influenced by the following considerations:

- The fatal damage rate must be less than 10(-10)/hour.
- The deployment should be transparent to the users, i.e. failure detection and isolation strategies should be independent of where the equipment is located.
- The deployment should not impose constraints on the allocation of tasks within an application processor such as SIFT, or in the bus controller, e.g. the assignment of a set of processors to service a bus should be independent of the location of the processor.

These requirements can certainly be satisfied if the system elements are deployed in such a way that a single damage event will not disable more that one element of a redundant set. Although this may be overkill, in most cases (depending upon the probability of damage), it is recommended as the deployment strategy for the advanced architecture.

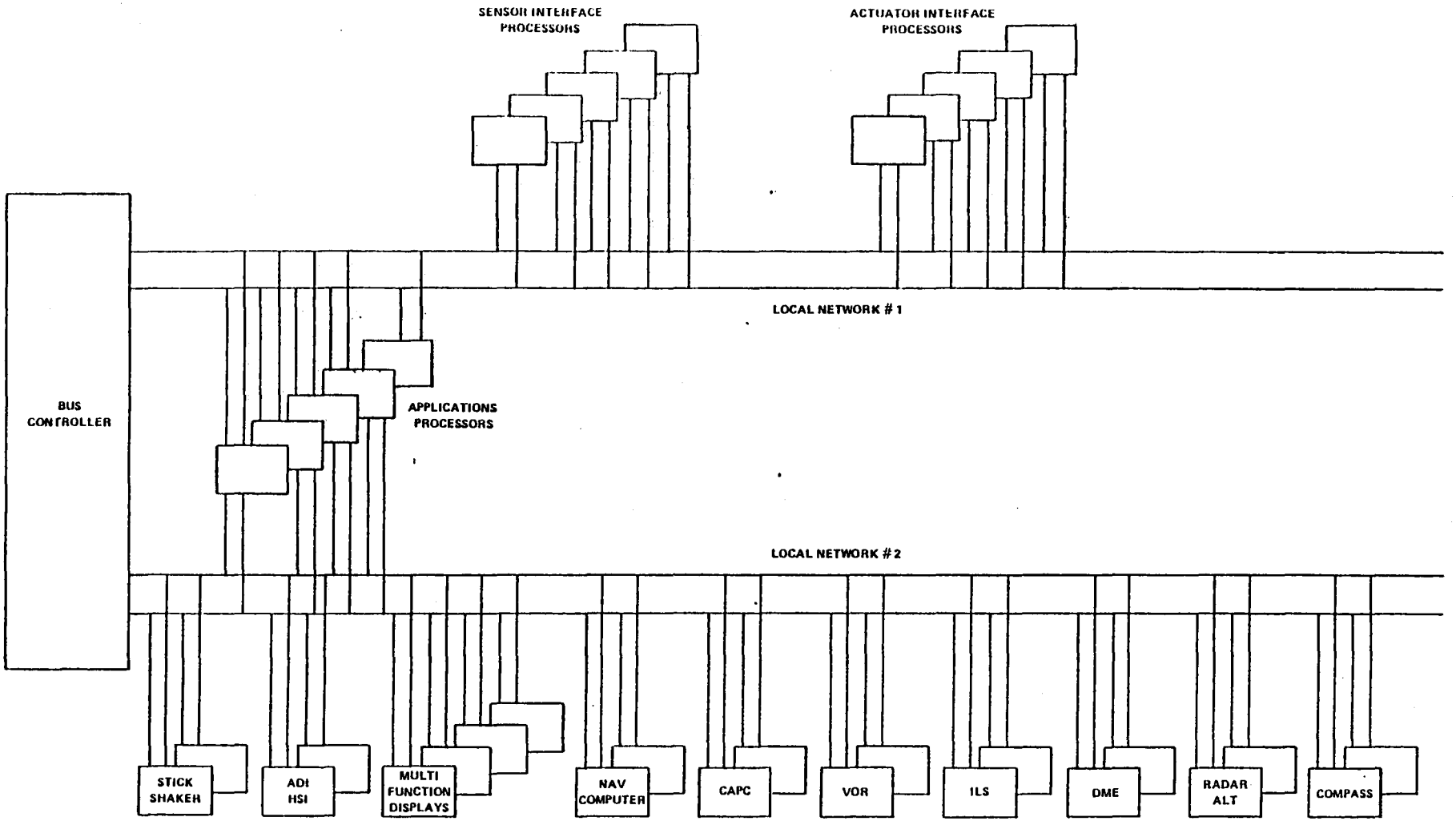


Figure 30 Advanced Flight Control System Structure

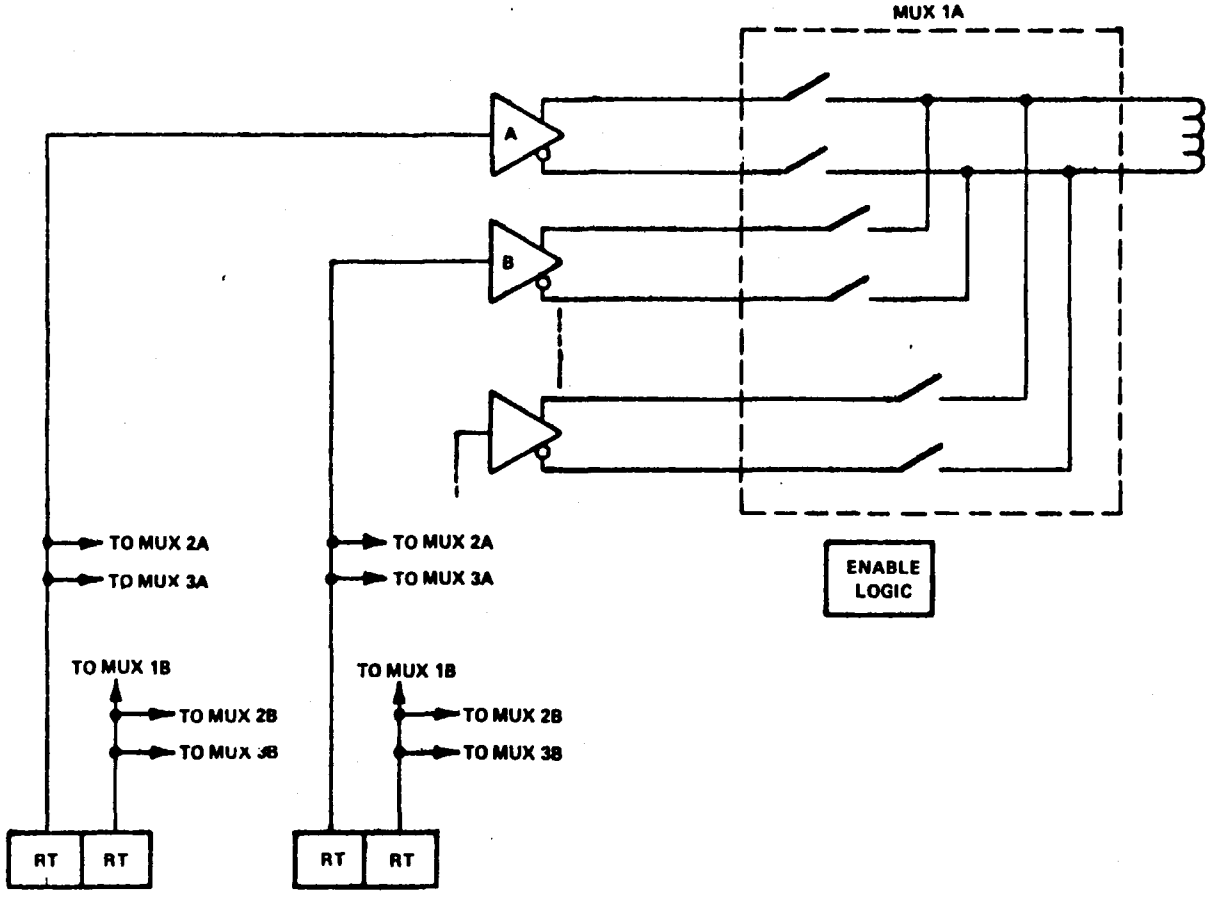


Figure 31 Multiplexer Arrangement

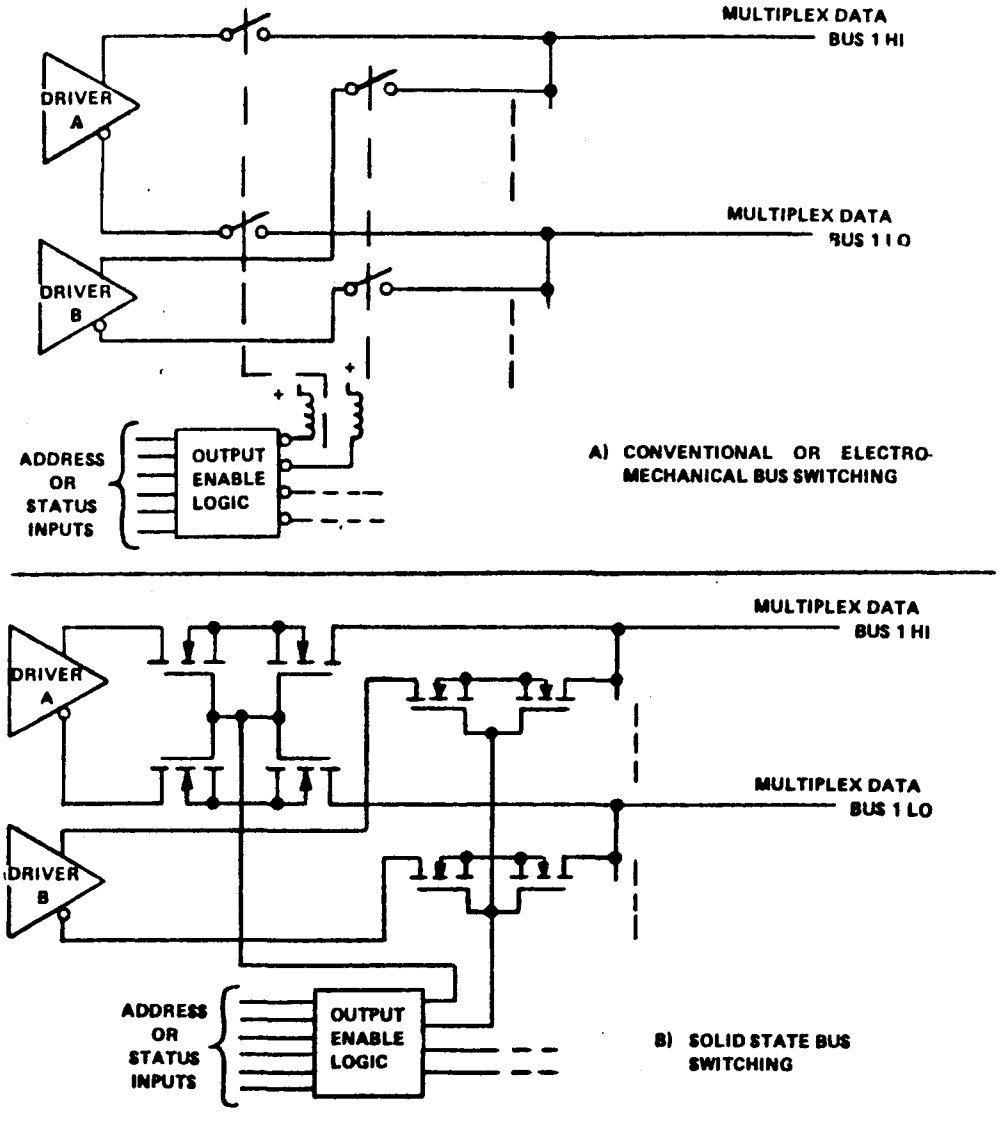


Figure 32 Methods of Switching Multiplex Data Busses

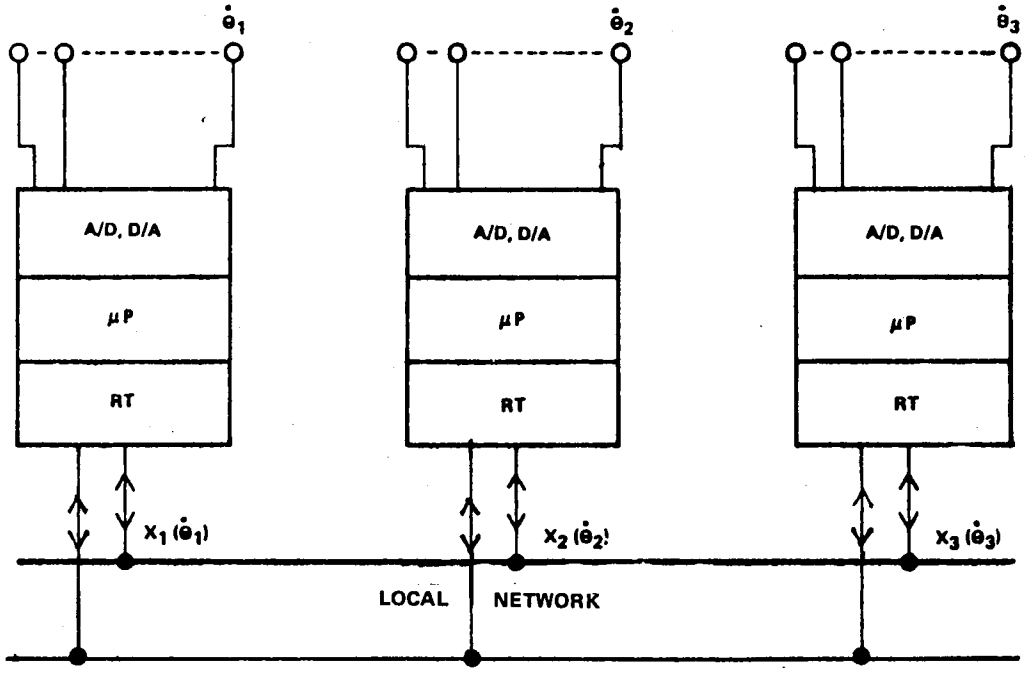


Figure 33 Sensors/Sensor Interface Processors

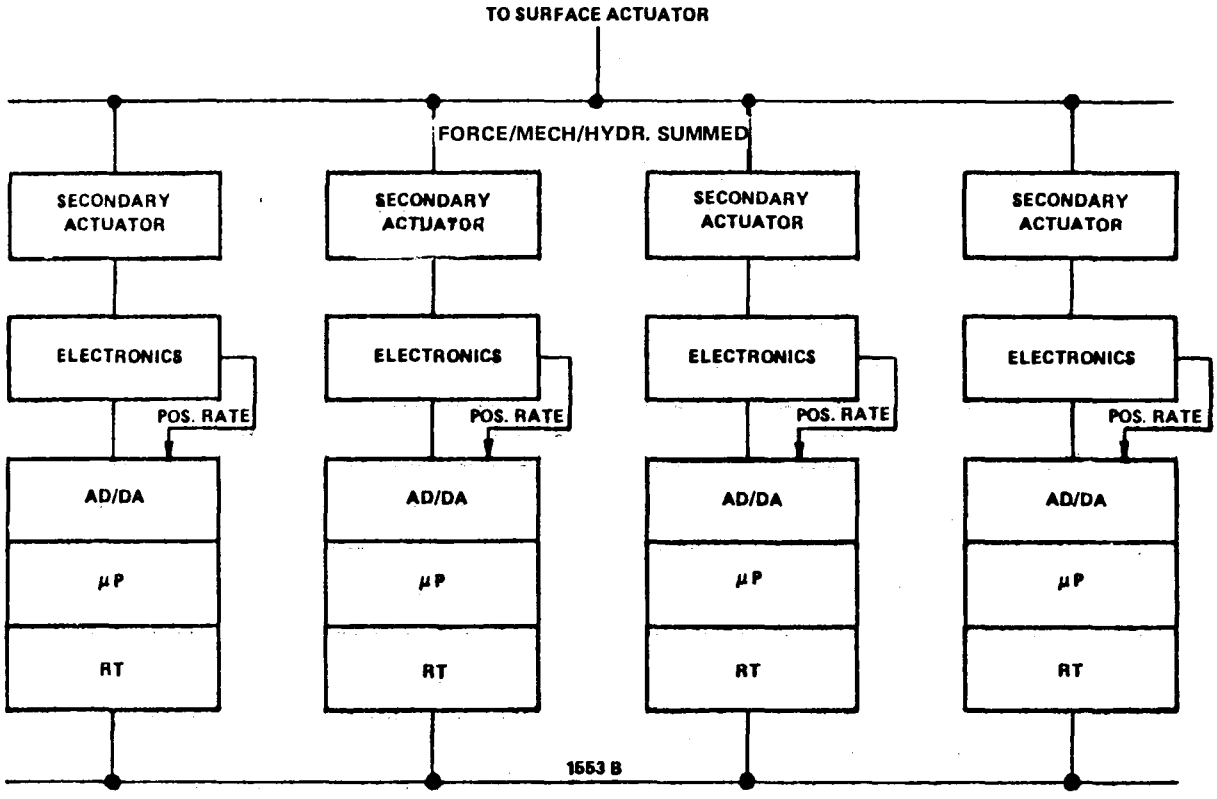


Figure 34 Actuators/Actuator Interface Processors

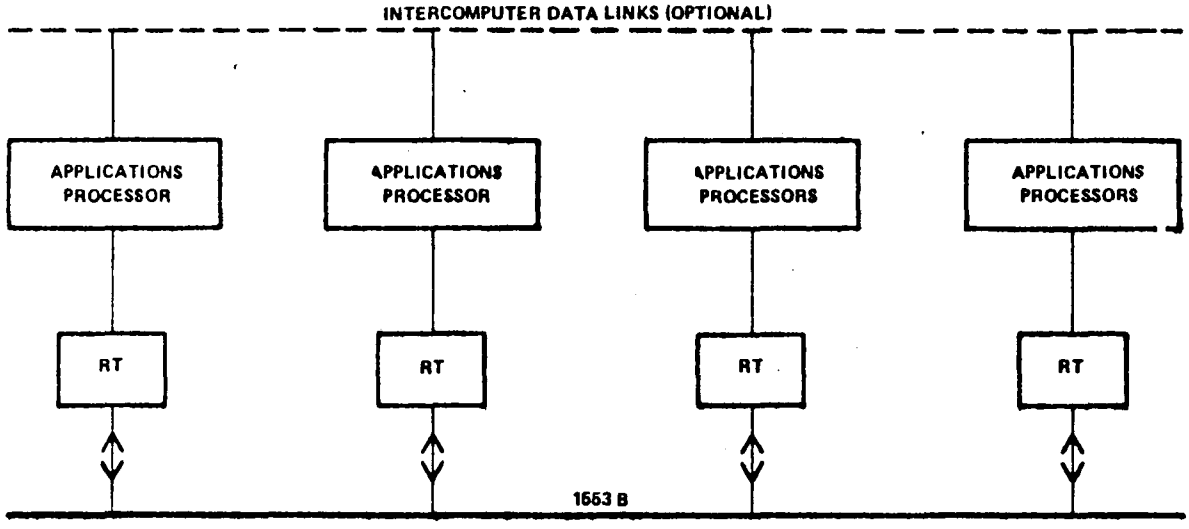


Figure 35 Applications Processors

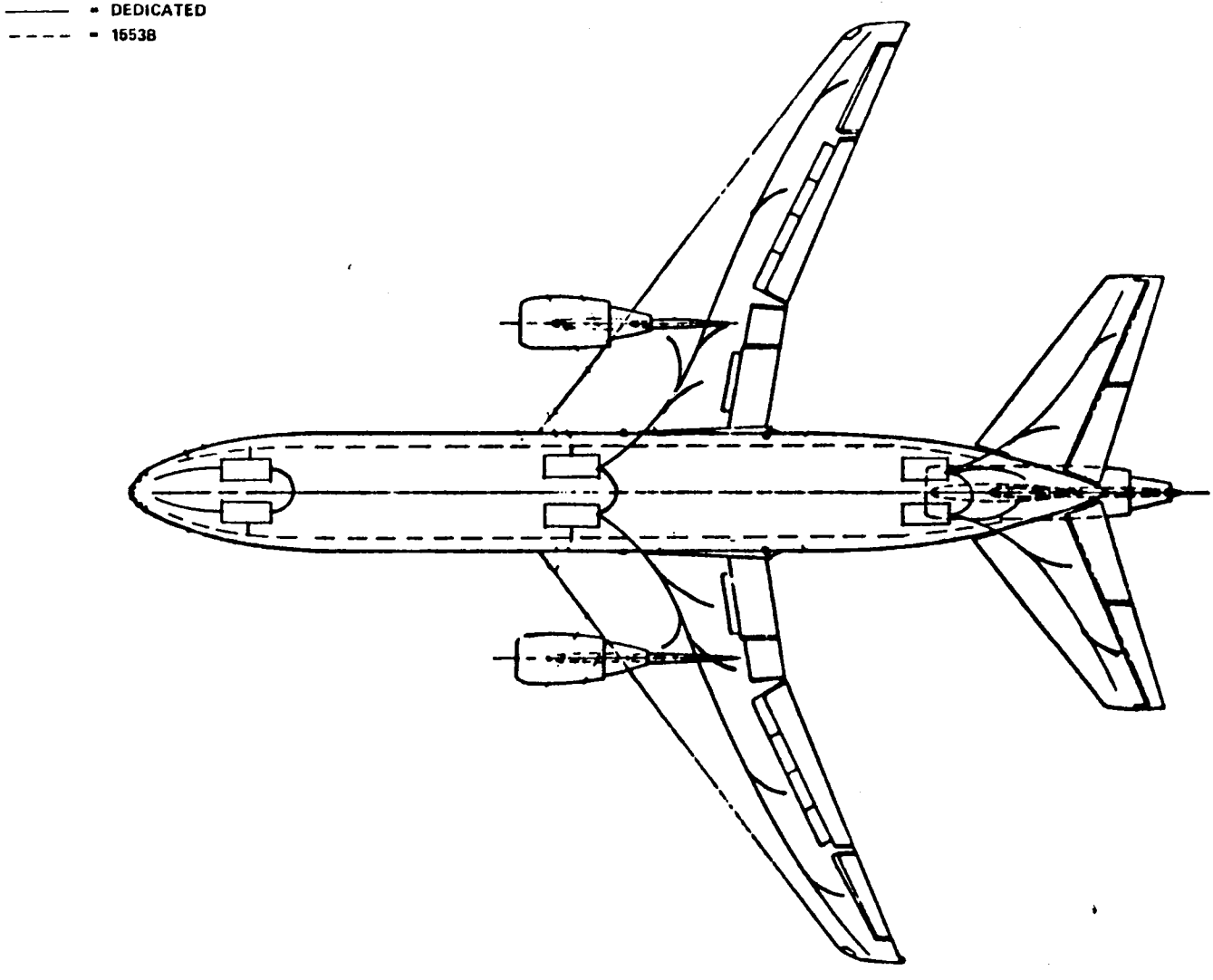


Figure 36 Bay Configuration

6.0 PARALLEL PROCESSING

6.1 Introduction

Most, if not all, digital flight control computations are processed sequentially. While sequential processing offers the advantages of unified software under the control of a single Executive, it creates a number of problems:

1. The CPU must be fast enough to execute the maximum set of computations, in sequence, in a prescribed period of time. Thus, the time required tends to increase linearly with the number of computations.

2. Software programs can be interactive in unexpected ways due to software errors or hardware faults.

3. The interaction of software, whether by design or error, imposes an additional burden on software validation. It is necessary to validate the potential interaction of each program as well as the program in isolation.

In order to overcome these problems the alternative approach of parallel processing was investigated for this study. Parallel processing offers significant potential benefits:

- By processing software tasks in parallel using multiple processors, the real time required is determined by the real time to execute a single task.

- Software programs are physically isolated. While there may be some areas of interaction, e.g. shared data, the interaction is minimal and, hence, relatively easy to validate. Moreover, a large proportion of faults and even software errors will affect only the errant processor and will require less validation, as a consequence.

- The distribution of tasks among smaller processors affords an improvement in reliability due to a) increased reliability of the smaller processors and b) the potential for cross-strapping.

- The distribution of tasks among smaller processors minimizes the effects of single faults on the total system. Thus, if control could be executed, in parallel, by axes, then loss of a single processor would only affect a single axis.

- The distribution of tasks among smaller processors results in smaller, more manageable, software programs.

In summary, the potential benefits of parallel processing are:

- improved real time
- simplified software
- simplified validation
- improved reliability
- growth capability
- improved software maintenance

It remains to be seen whether and to what extent these benefits can be realized in the flight controls application, and what the penalty is in additional hardware.

6.2 Feasibility of Parallel Processing for Flight Controls

Present and projected advances in microcircuit technology make the employment of large numbers of microprocessors in an aircraft technically and economically feasible. We anticipate, in the near future, inexpensive, single-chip microprocessors with self-contained memories and speeds comparable to todays' bit-sliced minicomputers. The availability of cheap and compact computing elements together with the potential benefits cited previously make parallel processing an attractive candidate for flight control applications.

In this section the feasibility of parallel processing for flight controls will be demonstrated. We note, in this connection, that parallel processing is implicit in the distributed system which disperses sensor, application and actuator processing. The concurrent processing of I/O and control laws is a standard practice even in conventional systems that employ, for example, DMA as autonomous I/O controllers, and it requires no further justification here. Thus, it only remains to demonstrate the feasibility of parallel processing within an applications processor.

6.2.1 Parallel Applications Processing

The objective of the parallel processor is to conserve real time by executing tasks concurrently. Relative to the flight control application our investigation of parallel processing was directed at the following issues:

- Can an algorithm be classified by the degree to which it lends itself to parallel processing?
- What is the connection between real time improvement and the number of processors used?
- What are the characteristics of the "ideal" parallel processor?
- What impact does parallel processing have on error detection, fault isolation and redundancy management?

No attempt was made to quantify the impact of parallel processing (i.e. the distribution of large software tasks into smaller, independent tasks) on software and software validation. Although we believe that the distribution and concurrent execution of software tasks will greatly simplify the software effort, a quantitative assessment of these benefits would not be credible at the present time. To be convincing, an evaluation would require a comparison study of software design and validation techniques and costs for conventional and parallel systems. In any case, it would be exceedingly difficult to assess conventional software costs inasmuch as the benefits of many software design procedures are largely subjective.

Classification of Algorithms

In general, a large class of algorithms lend themselves, in various degrees, to parallel execution. To characterize these algorithms we made numerous attempts to formally define a parallel process and in such a way that the definition coincided with common usage and, at the same time, provided a meaningful distinction between parallel and other processes. The effort was unsuccessful. Instead, we give an informal definition that, at least, highlights the distinguishing features of parallel processes in the context of the present study.

Definition

A "process" is a program executed on a CPU.

Definition

Two processes are "parallel processes" if, when executed on distinct CPU's,

- both processes can be executed concurrently and
- the computed outputs of either process are inaccessible to the other during their respective executions

We note that the above definition does not preclude a processor inputting from a source different from the other processor while it is executing, e.g. it can input from a remote terminal. Nor does the definition preclude outputting at any time during execution provided that the outputs are not made available to the other processor.

The definition can be extended to more than two processes in an obvious way, i.e all processes can be executed concurrently and the computed outputs of any process are not accessible to the other processes during their executions. According to this definition parallelism is not associative, i.e. if processes, P1 and P2 are parallel and P2 and P3 are parallel it does not necessarily follow that P1 and P3 are parallel. This is illustrated in Figure 37 where P1, P2 and P3 represent filters in a flight control computation. We note that this result conforms to common usage.

An interesting feature of the definition of parallel processing is that it is not explicit regarding the correctnesss of the resultant outputs. According to the definition P1 and P2 could be parallel processes even though P1 followed sequentially by P2 yielded a different output than when P1 and P2 were executed concurrently. This is illustrated by tandem filters in a flight control computation. The penalty paid for concurrent execution is a transport delay, which may or may not be acceptable.

From the standpoint of flight controls there are two potential penalties associated with parallel processing:

- the introduction of transport delays and
- real time and hardware overhead to support concurrent execution.

Transport Delay

Before assessing this penalty let us consider the transport delays of a sequential, digital process:

1. If the computation is iterated every T seconds, then the output sample and hold circuit introduces an effective time delay of T/2 seconds. This is the price one pays for digital processing.

2. The time delay between imputting a sensor and outputting the surface command. This includes computational delays. Minimizing this delay is the reason that data refresh rates should be at least 4 times greater than the iteration rate of the sensor subsystem.

As illustrated by the previous example, parallel processing could introduce an additional transport delay which is, effectively, an extension of the time between inputting a sensor and outputting to an actuator. In our treatment of parallel processor configurations every effort was made to eliminate or at least minimize this time delay while no attempt was made to improve upon the inherent time delays of the sequential process.

Distribution of Tasks

For the purposes of this study a "parallel processor" is a collection of distinct processors that execute their programs concurrently. A simplified version of a parallel processor is shown in Figure 38. Referring to the figure, a flight control computation is partitioned into subtasks and these are distributed among the microprocessors for execution. Most, but not necessarily all, of the subtasks will be parallel processes and can be executed concurrently without introducing a transport delay. Before commencing a subtask, each microprocessor fetches the appropriate input data from a common memory using a dedicated interprocessor link for this purpose. After completion of the task the microprocessor stores the results in the common memory for later access by other processors. Access to the local network is provided by a remote terminal (not shown) that exchanges data between the bus network and the common memory.

Two extreme examples of the distribution and execution of tasks in a parallel procssor are shown in Figure 39. Initially, three processes, P1, P2 and P3 are executed, in that order, in a sequential processor during a frame of duration, T. Each process is then assigned to a distinct microprocessor. If the processes are independent (i.e. parallel) in the sense that P3 does not require an output from P1 or P3 then the processes can be executed concurrently without introducing an additional time delay.

If, on the other hand, these processes are dependent then they must be executed sequentially (as in arrangement B of the figure) if an extraneous time delay is to be avoided. The arrows indicate the transfer of data from the output of one process to the input of another.

The point to be made here is that any flight control computation can be partitioned into subtasks and executed on distinct microprocessors without introducing extraneous time delays. The fact that some tasks may be executed sequentially does not necessarily diminish the real time benefits afforded. In this connection we note that both distributions provide, at least in theory, the same reserve of real time for additional processing. The differences in the two approaches are:

- each of the processes of arrangement B must be as fast as the sequential processor;
- arrangement B requires data transfers within a frame, which increases the overhead penalty.

Experience has shown that a substantial proportion of flight control computations can be partitioned and executed concurrently without introducing a significant, additional time delay.

Example 1

In conventional flight controls, pitch, roll and yaw axis computations are relatively independent. Thus, the distribution of these computations and their concurrent execution in distinct microprocessors would not introduce extra time delays.

Example 2

This example demonstates that some additional time delay may be unavoidable. An outer loop consists of two computations A, followed by B. A inputs the sensors and B outputs to the inner loop computation, C. We assume that the outer loop is iterated every T seconds and the inner loop, every T/2 seconds. The most efficient (from the standpoint of real time) concurrent execution of these tasks is shown in Figure 40. In this distribution CPU #1 executes the outer loop every T seconds and CPU #2 executes the inner loop every T/2 seconds.

From the figure it can be seen that the concurrent execution contributes an additional time delay of T/2 seconds, approximately. Of course, this time delay could be reduced by executing the complete

outer-loop every T/2 seconds but at the unacceptable expense of additional computations. Fortunately, the ratio of outer-loop to inner-loop iteration rates is greatly in excess of a factor of two, in practice. Since the extra time delay can never exceed T/2 seconds, the resultant effect on outer-loop dynamics would be insignificant.

2) Overhead Penalty

The real time benefits of parallel processing are measured by the reserve of real time available for additional computations (as indicated, for example, in Figure 39). Unfortunately, there is an associated real time overhead penalty that could seriously reduce the effectiveness of the parallel processor.

To assess this penalty let us consider n tasks, P1, P2, ...Pn, executed in a single CPU. We assume that the average time to execute a single task is T. We now assign each of these tasks to a distinct processor. For comparison purposes it is assumed that each of the n processors is identical to the original processor.

If the n tasks are now executed we will observe that each processor takes slightly more real time to execute its assigned task than the original processor. This is due, of course, to the real time overhead. In general, this overhead is due to:

- data transfers over the interprocessor link,
- executive programming requirements.

If

δT = average wastage time of a parallel processor executing a single task

then each processor requires, on the average, $T + \delta T$ to execute its assigned task. Thus, the total time required by the parallel processor to execute all of the tasks is $nT + n\delta T$, as compared with nT for the original processor.

We define the inefficiency of the parallel processor by the ratio

$$r = (nT + n\delta T)/nT = 1 + \delta T/T.$$

We interpret this to mean that it takes r processors, executing concurrently, to compute a task in the same time it takes a single, sequential processor. For example, if $r = 2$ then each parallel processor requires twice the computing power of a single sequential processor.

Estimating Efficiency of the Parallel Processor

In this section the inefficiency, r, will be estimated for several data exchange protocols.

Let

T = average time to execute a single task in a sequential processor

αT = average additional time to execute the task in a parallel processor

n = number of tasks = number of microprocessors.

In general, the wastage time, δT, will include

- time to input and output over the interprocessor link
- additional time required by the parallel processor Executive.

Worst Case Access Example

In the worst case the microprocessors will demand access to the interprocessor link simultaneously. Since only one microprocessor can be serviced at a time and a processor cannot execute until it fetches input data, all processors in a waiting line are idle. This is depicted in Figure 41. From the figure the total wastage is

1) $n\delta T = n(n + 1) T$

and, hence, the inefficiency ratio is

2) $r = 1 + \alpha(n + 1)$.

Observe that r is a function of the number of processors.

Random Access Example

In this case processor demand for access to the interprocessor link is random in time. As in the previous case it is assumed that processors in the waiting line are idle. The situation is depicted in Figure 42.

This is the classical queuing problem and is analysed in detail in (Ref. 13, PP 463-465). Using the terminology of (Ref 13), define

$1/\lambda$ = mean time between bus requests

$1/\mu$ = mean time to service a bus request

Q = mean queue length including the processor being serviced.

Then

3) $\mu/\lambda = 1/\alpha$

4) $Q = q + (1 - po)$

5) $q = n - (1 + \mu/\lambda)/(1 - po)$

6) $$1\text{-}po = \sum_{k-o}^{n-1} \frac{1}{k!} (\mu/\lambda)^k \sum_{k-o}^{n} \frac{1}{k!} (\mu/\lambda)^k$$

7) $\delta T/T = Q/(n-Q)$

8) $r = 1 + Q/(n-Q)$

Figure 43 is a plot of the inefficiency ratio, r, versus number of processors for several values of α. It remains, now, to estimate α for a flight control application.

Estimating α in a Flight Control Scenario

In order to estimate α the flight control software for the DC-10 stretch airplane was analysed for distribution and execution in a parallel processor. The single thread software tasks were originally subdivided into five major modules, as shown in Figure 44. This figure also shows the memory and real time required for each module using the Bendix BDX-930 computer. The resultant distributions of tasks for parallel processing are given in Figure 45. The memory and real time requirements are given for the BDX-930 and the TMS 9995 microprocessor. The number of I/O and interprocessor data transfers are shown in Figure 46.

To be conservative we assume

- serial interprocessor data link
- 30 microseconds to transfer a single word
- real time to transfer, in sequential processor, is negligibly small

In accordance with out previous groundrules, we assume that each microprocessor has the same computing speed as the BDX-930. Because of the fixed transfer time and the high speed of the BDX-930 the resultant estimate of wastage will be extremely conservative.

From Figure 45 it can be seen that the average real time to compute a module in the BDX-930 is 5.7 milliseconds. From Figure 46 there are 66 data transfers or an average of 22 per module. Thus,

$T = 5.7$ milliseconds

$\alpha T = 22 \times 30/1000 = 0.66$ milliseconds

and, hence,

$\alpha = 0.12$,

From Figure 43 it can be seen that the inefficiency ratio for $\alpha = 0.12$ and four processors is

- 1.25 for worst case access
- 1.15 for random access

Thus, there is a 25% reduction in efficiency for the worst case access and 15% for random access.

In practice, of course, the modules will be executed in microprocessors having considerably less speed than the original, sequential processor. As an illustration of this differential we included the corresponding real time for execution in a TMS 9995 microprocessor in Figure 45. From this figure it can be seeen that the maximum time to complete a module is 34.78 milliseocnds. Since the frame time is 100 milliseconds there is ample reserve time available for additional computation and to absorb wastage.

We note that, had we used the TMS 9995 to estimate wastage, the result would have been

$$\alpha = .66/28.9 = 0.02.$$

6.3 PARALLEL PROCESSING CONFIGURATION

The general characteristics of the parallel processing system proposed here are depicted in the block diagram of Figure 47. This configuration is described later in greater detail, however, it is presented here in order to provide an overview of the proposed parallel processing configuration.

Parallel processing systems require (rapid) access to data throughout the system to a greater extent than most networks; hence, the need for a shared memory system. One method of memory sharing provides a single common memory system with either no private memory or only private (ROM) program memory. In general, the degree of memory contention in such a system becomes a limiting factor. Consequently, the three alternative memory sharing techniques depicted in Figure 48 have been considered. In Figure 48a, arbitration logic is centrally located at the shared common memory. In this configuration two accesses are required to the interprocessor bus for each transaction, e.g. one access is required to transfer a copy of the data from the source processor to the common shared memory and a second access is required to transfer this data to the destination processor. This approach maintains the integrity of the source data since the destination processor cannot directly access it; the destination processor only has access to the common shared memory. In Figure 48b the shared memory is distributed throughout the system and a portion is associated with each processor in a decentralized manner. In this configuration only one interprocessor bus access is required since each processor has direct access to the shared memory local to every other processor. (Here, the integrity of the source data may be questionable in the presence of faults). In Figure 48c, the advantages of the distributed shared memory are maintained for shared variables while providing dedicated private memory for both the program memory (ROM) and private variables (RAM- scratchpad). Furthermore, hardware can be provided to limit and control access to specific segments for specific processors (the benefits of limited access control shall be evaluated in the next phase of this program). It is this last configuration, Figure 6-12c, which is proposed here.

In the selected shared memory configuration, a portion of the shared memory is physically associated with one processor but is accessible to all processors. Access to a processor's own private memory as well as its physically associated shared common memory is done locally while remote shared memory is accessed by means of transfers over the interprocessor bus. Since each processor in this system makes reference primarily to its local shared memory and only uses remote memory "sparingly", the system performances is not limited by the bandwidth of the interprocessor bus.

If the total shared memory (logical address space) exceeds the physical address space of any processor, a memory address mapping function is required. The map function provided here is useful, even if the total logical address space is less than the physical address space, in that it simplifies the required memory address space assignment.

Figures 49 and 50 provide details of the Application Processor and the Executive Processor. These two processors are identical except for MIL-STD-1553 Remote Terminal interface(s) provided in the Executive Processor, for external communications.

The resulting memory hierarchy consists of local, private (on chip microprocessor memories are now being introduced by manufacturers and are in the development plans of others) memory having both ROM and RAM memory as well as having provisions for off-chip expansion of the private memory. This off-chip expansion feature allows local monitoring and debugging routines to be located where they are easily deletable; this feature also provides growth capability. The microprocessor has access to its local shared memory via the memory address mapped under memory allocation control without utilizing the interprocessor bus. Access to remote shared memory shall be via the memory address mapped under memory allocation control which functions in conjunction with the interprocessor bus controller (arbiter) to provide conflict-free access.

The memory allocation control unit, in conjunction with the interprocessor bus controller, establishes the data path to the shared memory in each cycle by determining whether the local processor or a remote processor has access to the particular shared common memory segment. Requests for the interprocessor bus and use of shared memory initiate the action taken by these units. Hence, all processors are able to share portions of the physical memory. This allows a processor access to its own local memory (which is reserved primarily for its use) as well as allowing limited controlled sharing with other processors. The arbitration logic resolves any competition for the interprocessor bus and provides information to the memory allocation control unit so that the necessary address and data path is established between the source (destination) processor and the destination (source) memory.

The individual application processors are linked together by the single interprocessor bus which is here configured as a parallel bus consisting of the necessary address, data and control lines. Although the single bus structure places some constraints on the general purpose parallel processing system, this constraint is not significant in our applications. It only requires that a high majority of the processor's memory activity be to its local memory subsystem; this minimizes interprocessor bus requests and potential bus contention. In fact, the communications requirements of the system could be met by a serial link rather than a parallel interprocessor bus. An alternative serial link shall be considered during the next phase.

The arbitration and allocation algorithm selection and implementation details, i.e. test and lock functions (to prevent simultaneous access), will be finalized during the early hardware design phase. Techniques being evaluated for the arbitration and allocation algorithm include the rotating bus mastership approach and the master/slave executive/application processor communications approach. In the rotating bus mastership approach, bus control passes from processor to processor, with the present master required to wait for all succeeding requests to be serviced before regaining its position as master. This prevents interprocessor bus "hogging" that otherwise can occur in a fixed priority scheme. In the master-slave arrangement the executive functions as the master in controlling interprocessor bus communications.

6.4 Monitoring

The advanced architecture allows considerable flexibility for monitoring the parallel processor. One such strategy is:

- Output variables are monitored by the bus controller
- When a fault is detected the bus controller directs the affected parallel processor to isolate the fault.
- A failed microprocessor can be isolated by

  a) self-test

  b) comparison monitoring

Comparison monitoring could be performed continually or only when requested using the local network or a private network for interchange of data between parallel processors.

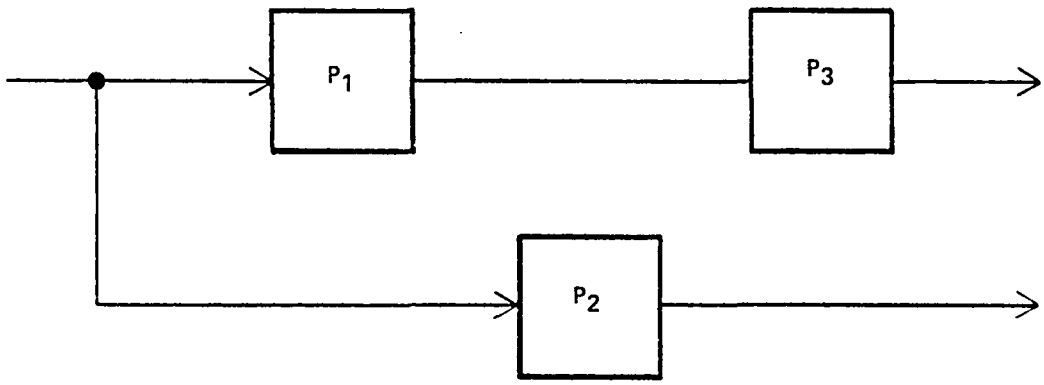


Figure 37 Non-Associative Character of Parallel Processing

(P_1 11 P_2 AND P_2 11 P_3 BUT P_1 11 P_3)

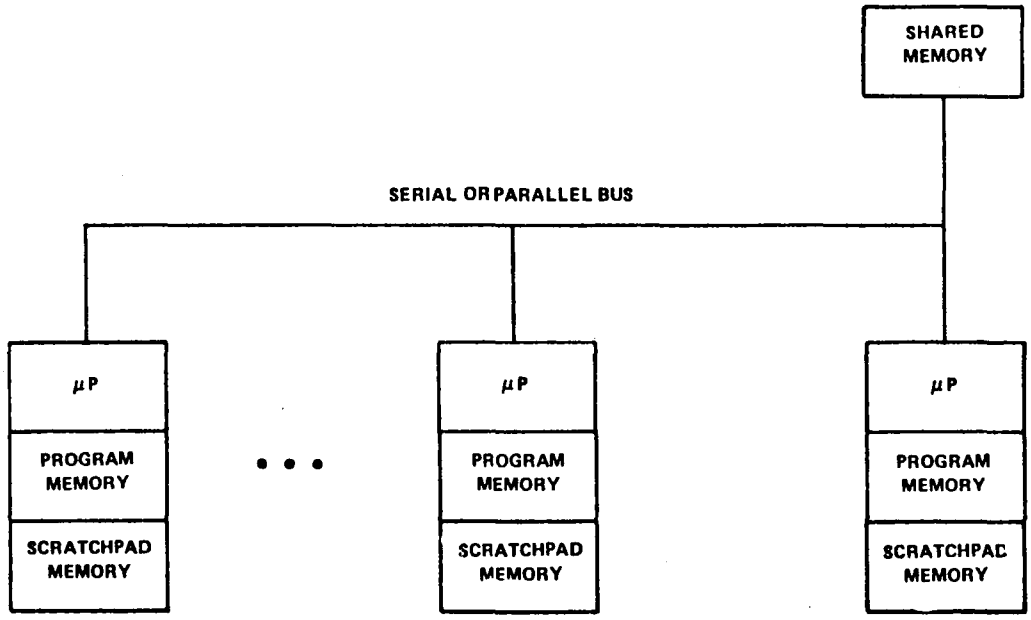
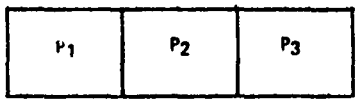
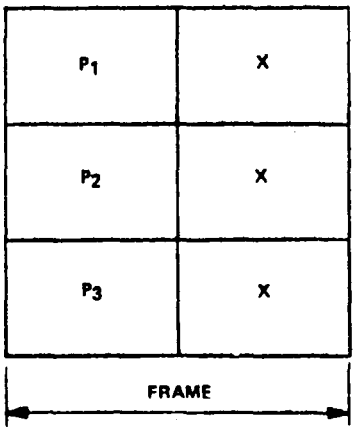


Figure 38 Candidate Parallel Processor

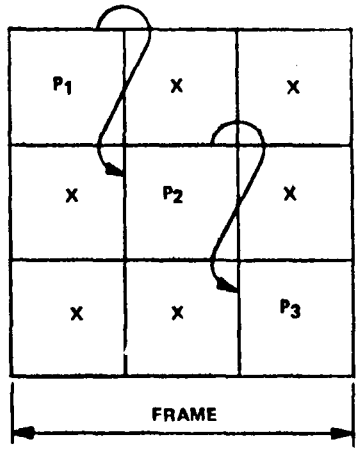


SEQUENTIAL PROCESS



PARALLEL PROCESSOR DISTRIBUTION OF TASKS

ARRANGEMENT A



PARALLEL PROCESSOR DISTRIBUTION OF TASKS

ARRANGEMENT B

X = AVAILABLE FOR ADDITIONAL PROCESSING

Figure 39 Parallel Processor Distribution of Tasks

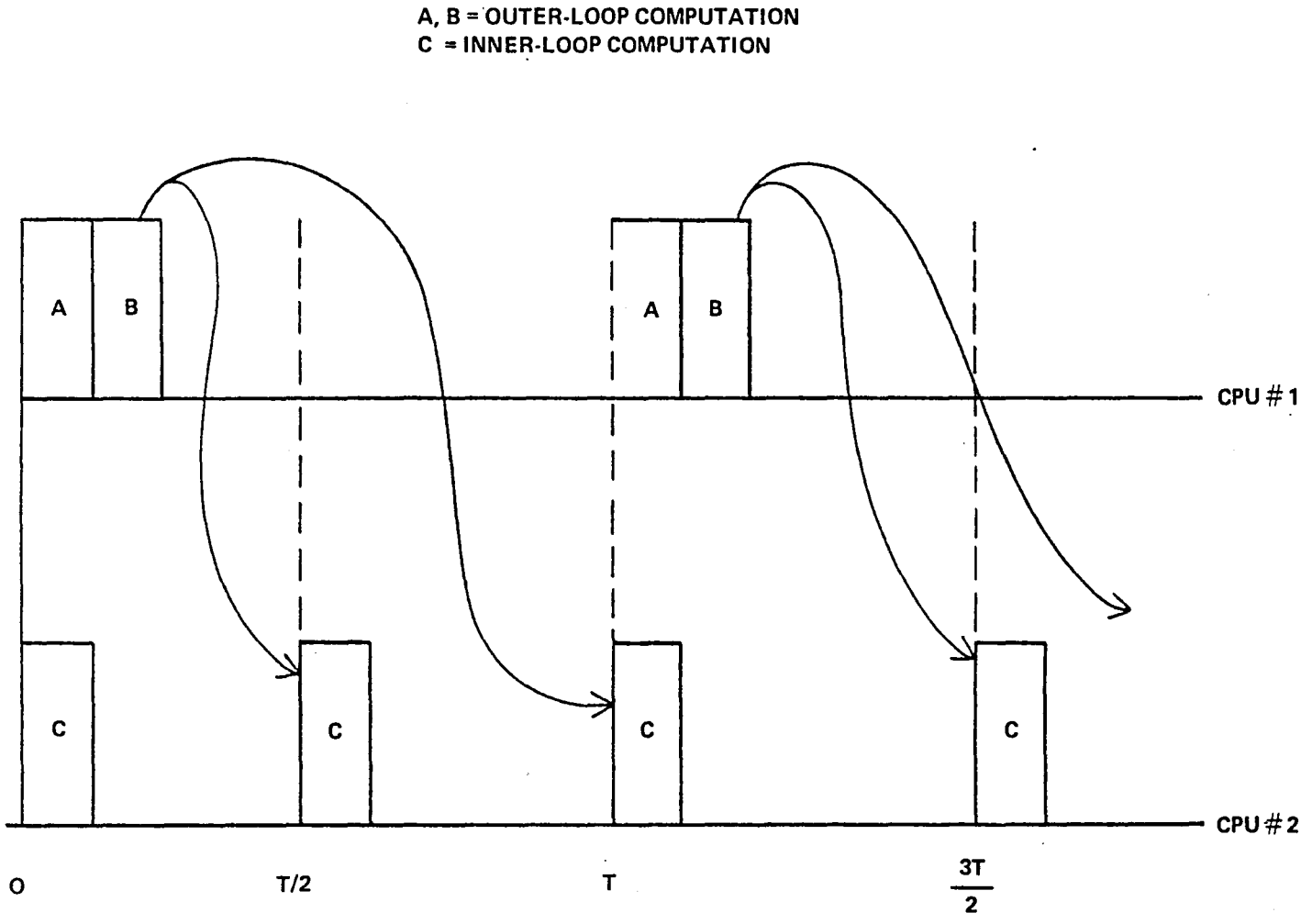


Figure 40 Outer-Loop/Inner-Loop Computation

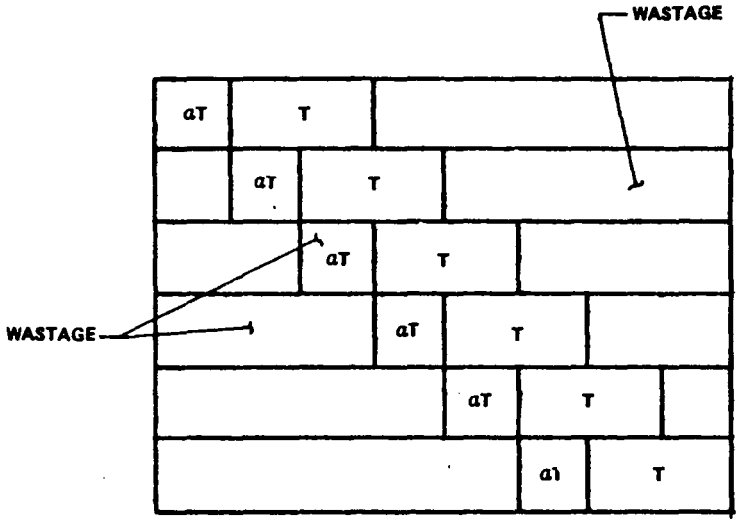


Figure 41 Worst Case Wastage Simultaneous Demand for I/O

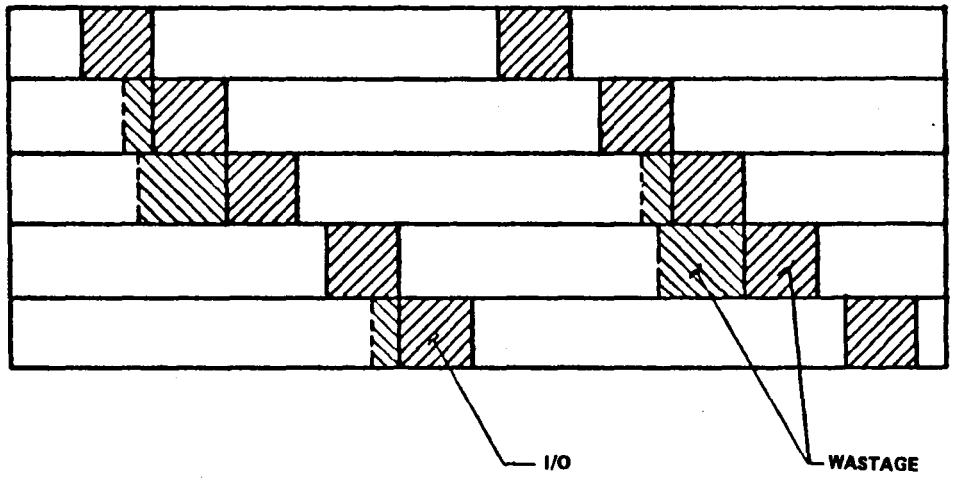


Figure 42 Wastage Randomly Accessed I/O

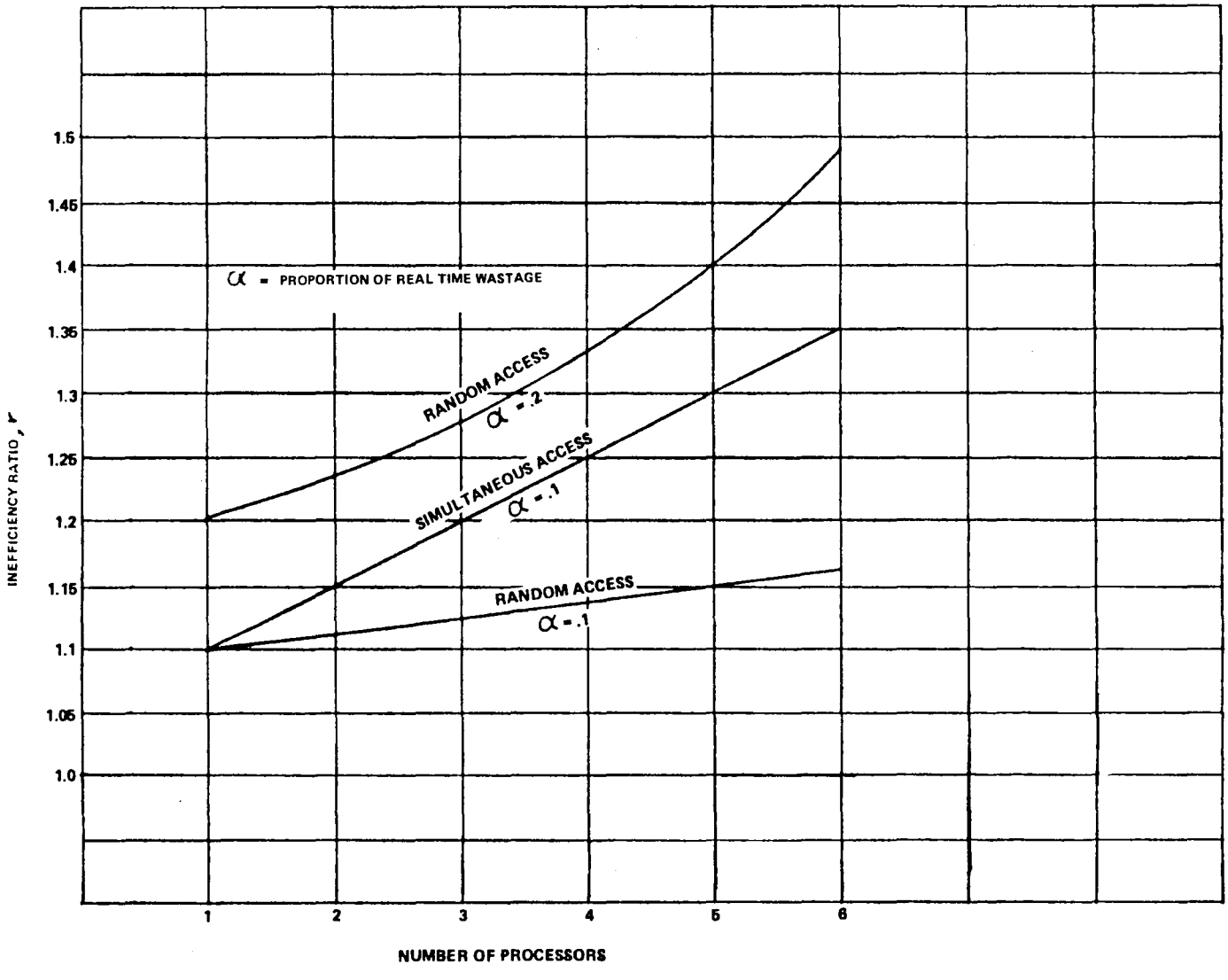


Figure 43 Parallel Processor Inefficiency Ratio Versus Number of Processors

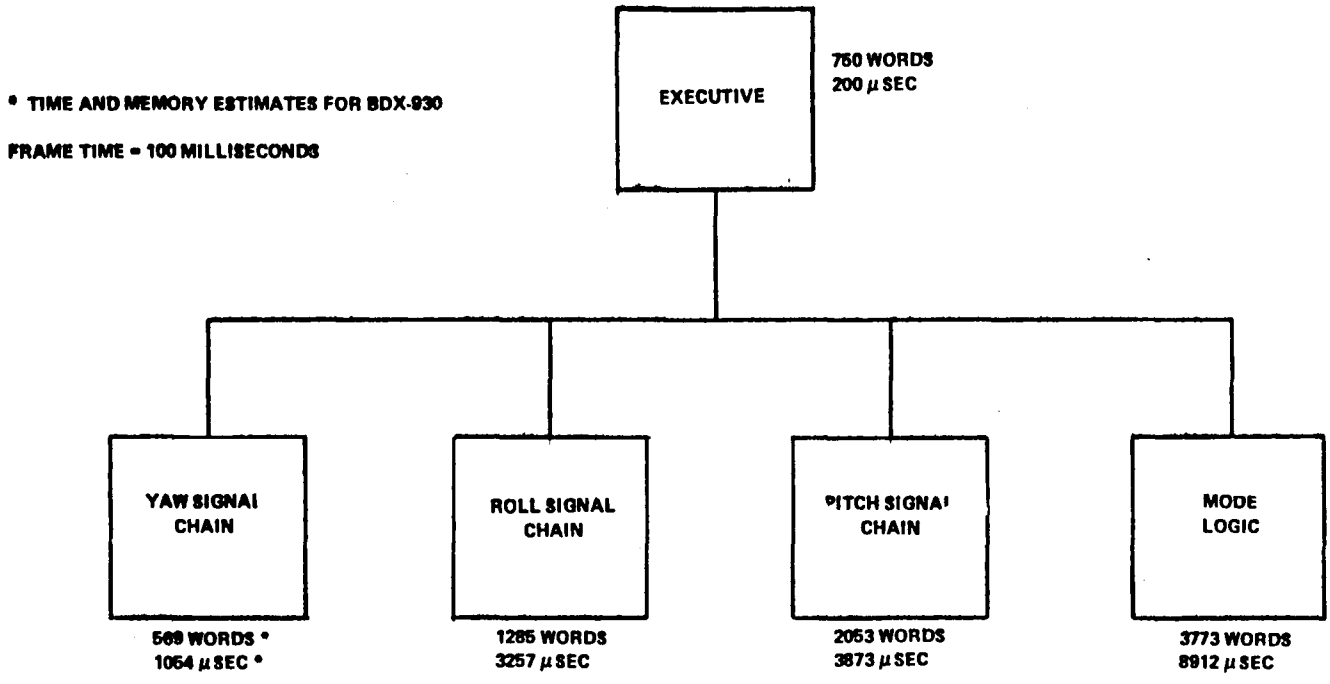


Figure 44 DC-10 Stretch Flight Control Software Modularization for Sequential Processing

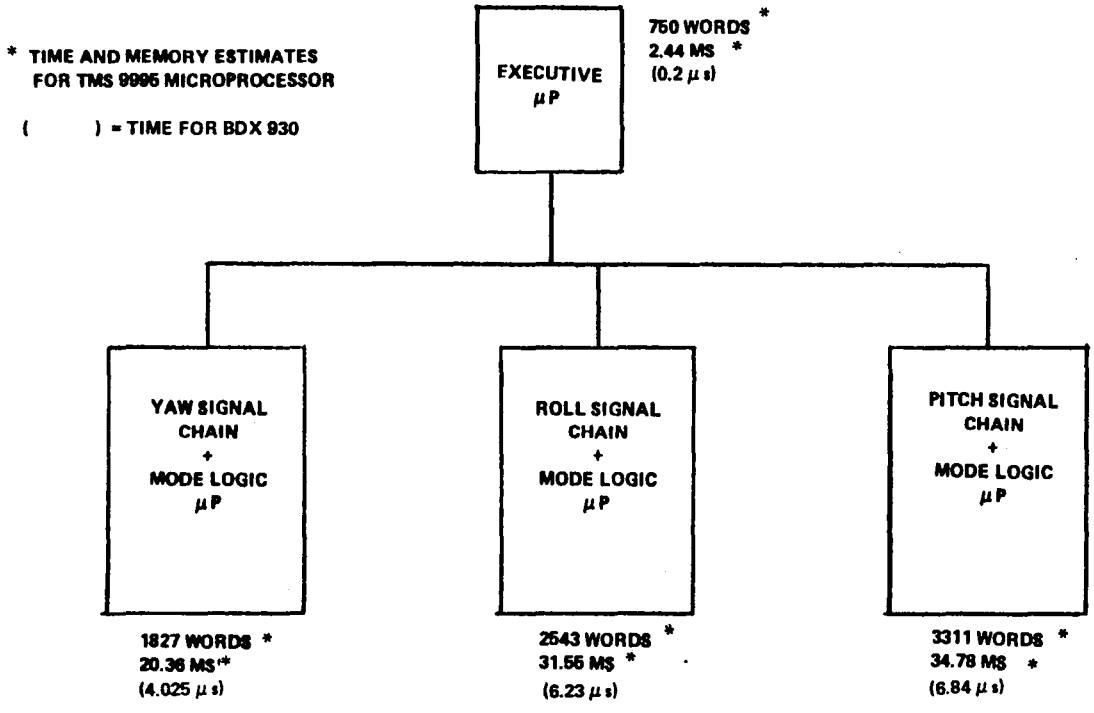


Figure 45 DC-10 Stretch Flight Control Software Modularization for Parallel Processing

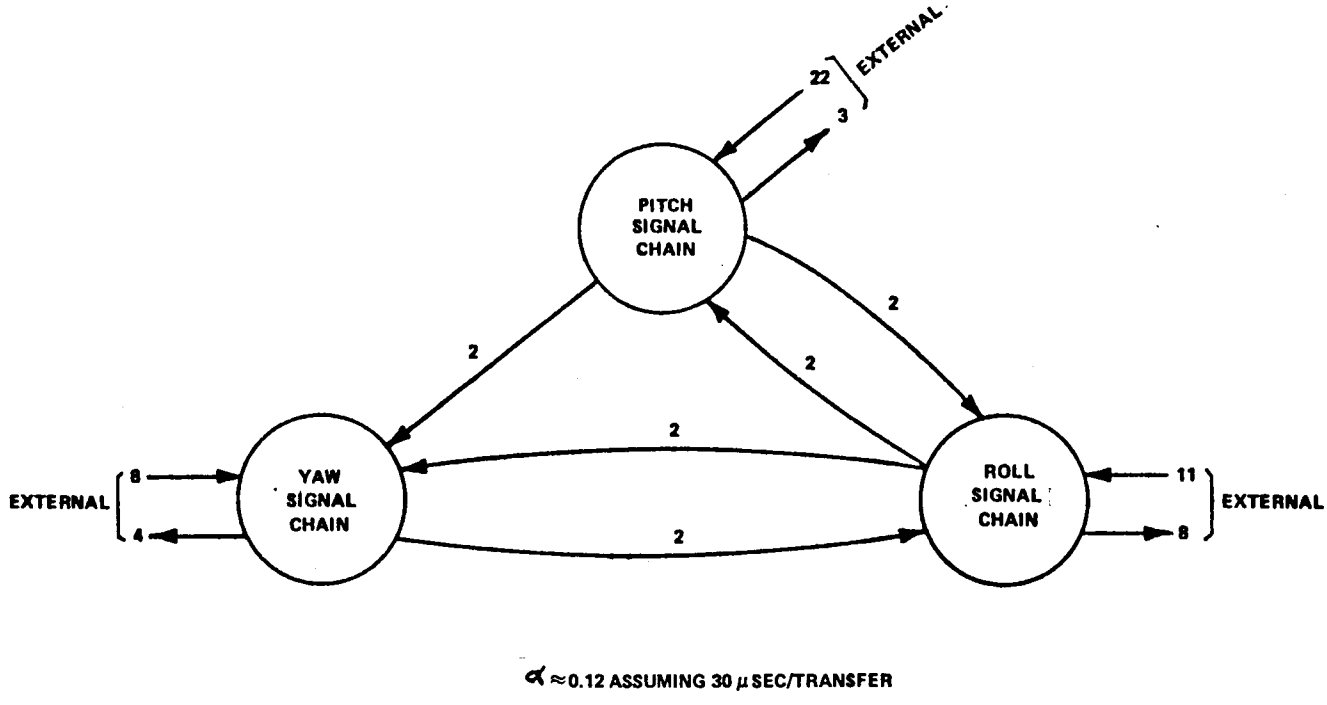


Figure 46 Interprocessor Transfers DC-10 Stretch Flight Control System

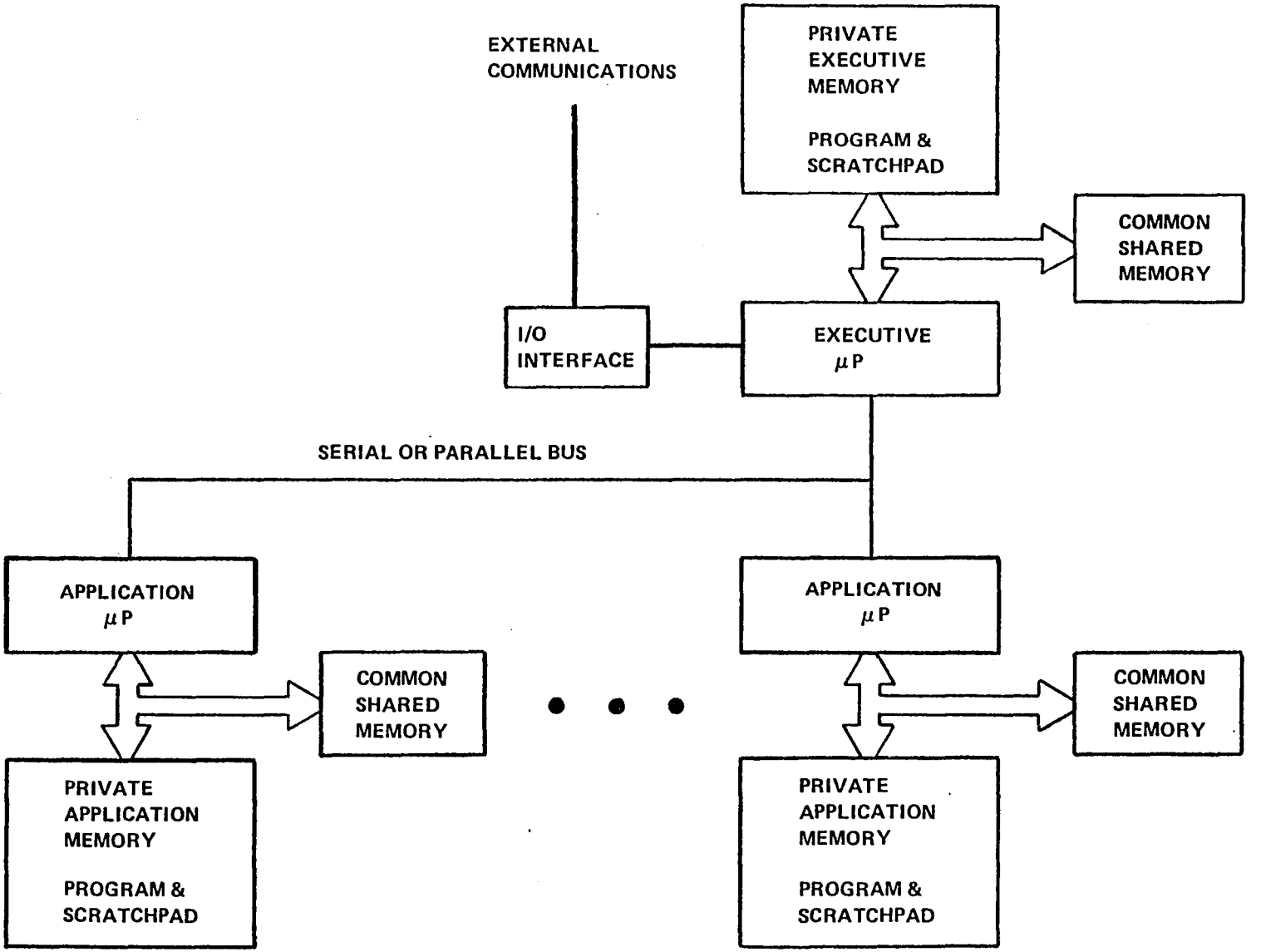


Figure 47 General Block Diagram Parallel Processor Configuration

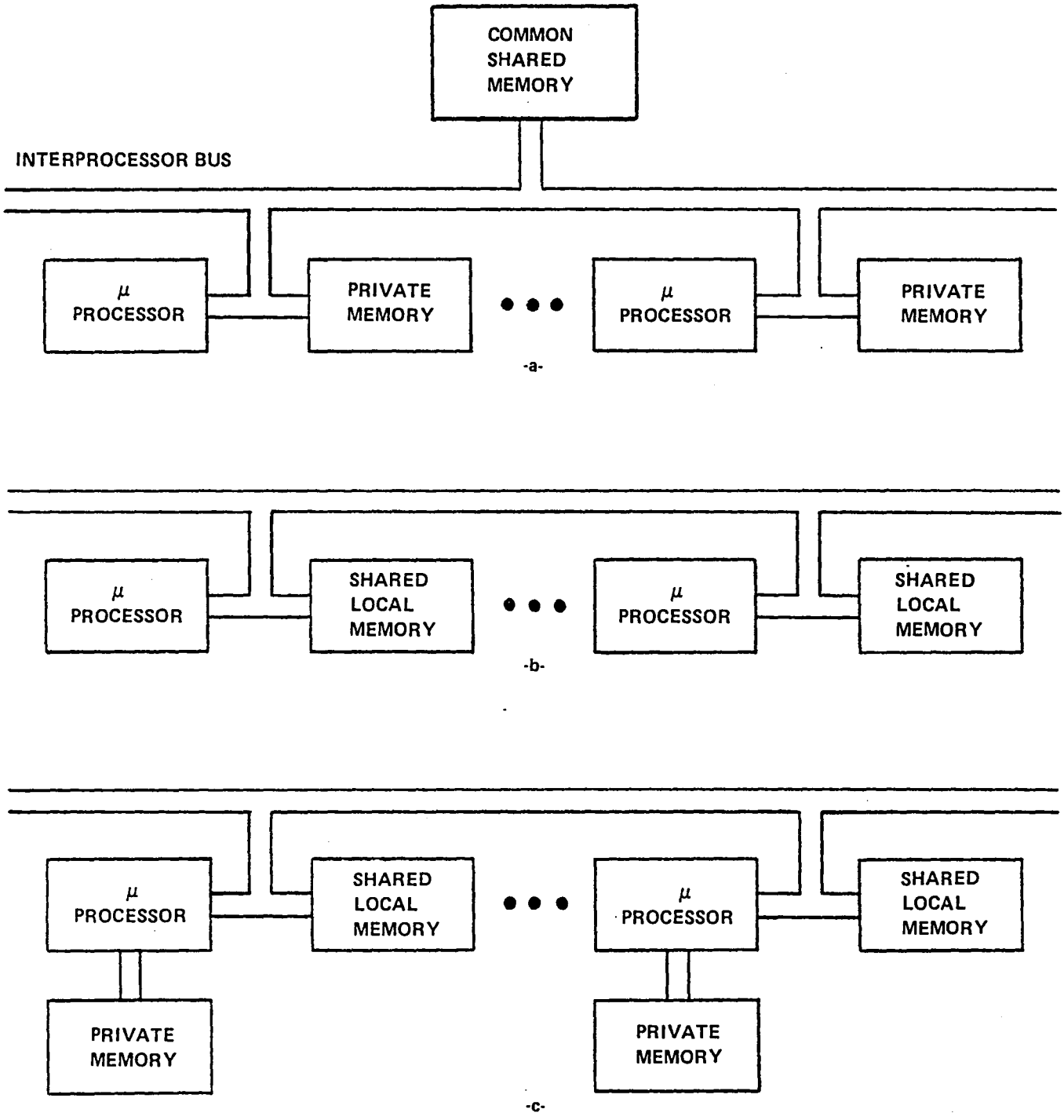


Figure 48 Memory Sharing

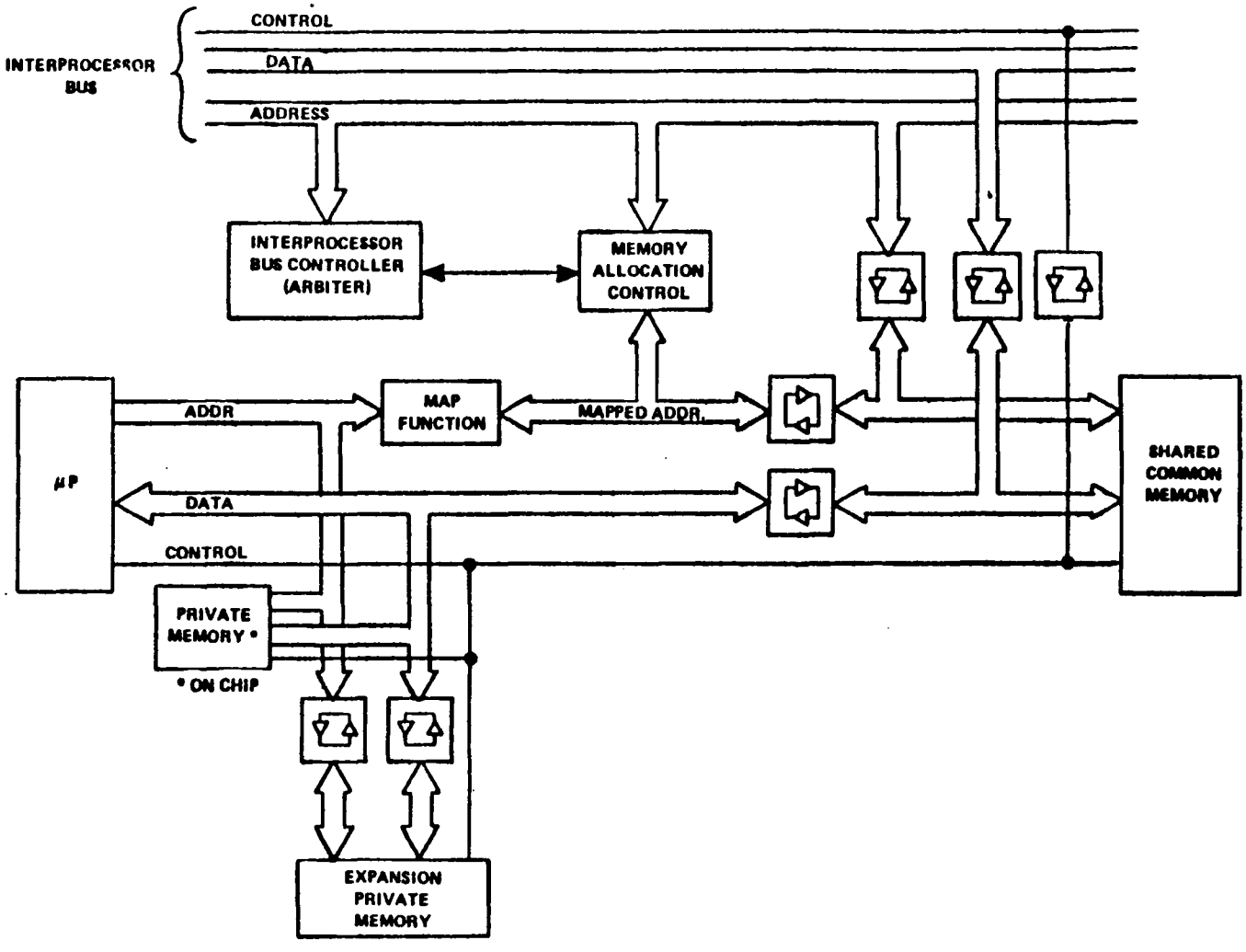


Figure 49 Typical Parallel Microprocessor Application Processor

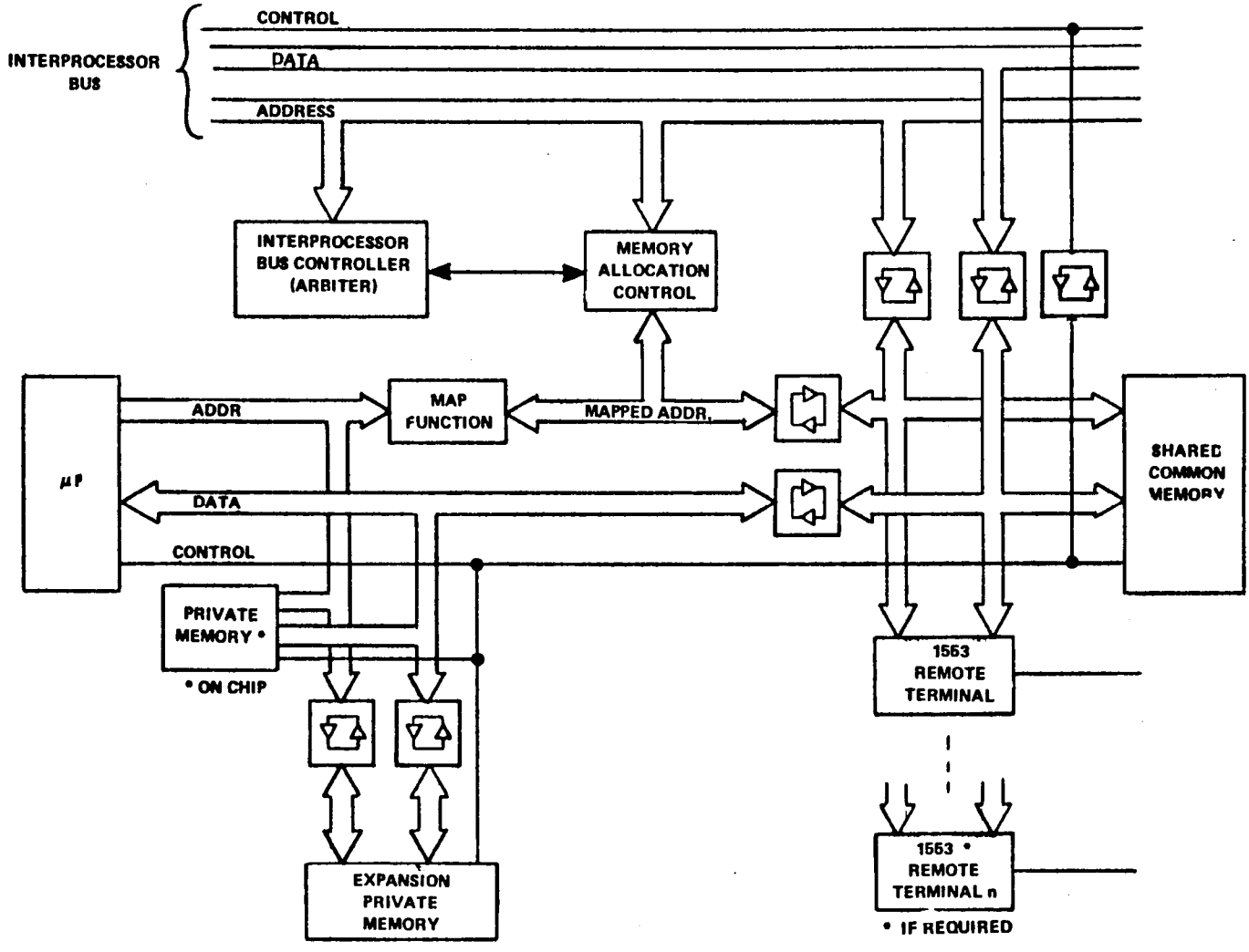


Figure 50 Typical Parallel Processor - Executive Processor

7.0 TRADE-OFF STUDIES

7.1 Introduction

One of the objectives of the present study is to seek new and innovative strategies in advanced flight control systems which would have significant advantages over conventional approaches and architectures in the specific areas of:

a. The ability to tolerate multiple faults without degraded operations.

b. A reduction of maintenance requirements to periodic actions which would facilitate dispatch capability with failed elements.

c. The ability to expand and/or modify functions without rearrangement of existing software or system interfaces.

The advanced architecture will be heavily dependent upon a variety of new technologies, some of which are identified in Figure 51. These and related technologies are further identified in Table 7, along with a brief summary of their projected impact on the Advanced Flight Control System.

Subsequently trade-offs in this section will emphasize, exclusively, the

- fault-tolerant
- periodic maintenance and
- expansion/modification

capabilities of the candidate architectures. Supporting technologies will be evaluated in this section only to the extent that they enhance these capabilities. As a consequence, some technologies will be ignored or only casually mentioned in this section even though their potential weight and cost payoffs may ultimately provide the major incentive for an advanced architecture. (Ref. 17)

The potential economies conferred by an advanced architecture are reduced hardware, software and maintenance costs, technology independence, expansion and modification capability and dispatchability.

Hardware Costs

These costs are measured in terms of the quantity and quality of subsystem components such as computers, communication networks and interfacing, electrical and hydraulic power requirements and weight. Indirect cost benefits are realized through lighter structures, fuel savings and refined operational procedures. One means of providing economy is sharing resources such as sensors and computers and by providing access to surviving elements. When evaluating economy the total system should be considered. For example, an architecture that is cost effective for flight control, which employs dedicated components and resources, may be a bad bargain in the long run since there is no sharing of resources with other subsystems. In fact, the non-accessibility of resources (even if available) has been the major stimulus for research in analytical redundancy.

As an indication of the potential economy of an advanced architecture weight reduction benefits were evaluated in (Ref. 17) for digital, fly-by-wire controls with a multiplexed communications medium. The weight reduction benefit of these technologies, alone, was over 800 lbs. for a large commercial transport, with multiplexing accounting for half of the total.

Software Costs

Software cost is measured in terms of design, documentation, configuration control and validation costs. Experience has shown that software is easy to produce but difficult and costly to document, validate and modify. It is unlikely that a large and complex software program can be produced with an error rate of 10(-10)/hour unless a rigid and costly discipline is imposed. At present the major efforts to produce reliable software are: rigid structure, modularization, mathematical proof, automated testing procedures. use of a standardized processor and a higher order language.

One of the benefits of the proposed architecture is its potential for simplifying system software through the use of standardized communication and data formats, and distributing and parallel processing. Since the architecture imposes no constraints on the computing element, it can accommodate standardized processors, as these become available, with a minimum impact on the system. Distributed and parallel processing offer the benefits of smaller, more manageable and validatable software modules which are physically as well as functionally independent. Parallel processing confers the additional benefit of improved real time capability.

We envision, eventually, that flight control systems will be designed for implementation in distributed, parallel processors. Computations will be tailored to this kind of implementation and, thus, may avoid some of the problems connected with transforming a sequential program to a parallel processor. The distribution of tasks and the use of standardized I/O will broaden the community of qualified designers and allow greater participation in the design and development processes.

Technology Independence

One of the most serious limitations of the conventional flight control system is its inability to accommodate advanced hardware element retrofits. Thus, the conventional system quickly becomes obsolete. Because the original design was based on customized interfaces and signal formats and because the design was heavily dependent on special features of the computers, actuators and sensors, performance improvements require significant and costly modifications to the original design.

The accommodation of new technology was a primary goal of the proposed architecture. In fact, it may be said that most of the technical risks associated with the advanced architecture were the results of this accommodation.

Expansion Capability

The architecture should have the capability to not only accommodate advanced hardware elements but to expand functions and add subsystems with a minimum impact on the system. Expansion capabilities must include software and hardware. Because of its rigid structure, the conventional flight control system, with its dedicated components and communication, can only expand within a limited envelope prescribed by its reserve of I/O, memory and real time. The proposed architecture, on the other hand, allows for an indefinite expansion which, in practice, is limited only by the number of terminals that can be connected to a local network and by bus bandwidth. The most significant impact of an added subsystem is on the bus controller software which must incorporate the new subsystem into the local network.

Maintenance Costs and Dispatchability

These costs are determined by component reliability, location and ease of access of components, frequency of maintenance actions, fault diagnosis procedures and the availability of spares. Trade-offs of these parameters will be given in detail in the next section.

It is appropriate to mention, at this time, the technical risks associated with the proposed architecture. During the study, technical risk did not disqualify an option unless the risk was judged to be totally unacceptable or the potential benefits did not seem to justify even a moderate risk. As a consequence, when it came to a choice between moderate risk and benefits the choice was always made for benefits.

Technical Risks

The technical risks have been identified throughout this report and, in all cases, methods for evaluating and surmounting them have been described. We include, here, a summary of these risks:

1. A 1553B bus for critical flight controls may be unacceptably vulnerable to single point failures due to damage by a babbling terminal.

2. The bus controller must be ultrareliable. Bus control processor, bus controller interfaces and bus control monitoring must support the 10(-10)/hour survivability goals.

3. Flight control system software can be efficiently distributed and executed in a parallel processor.

4. Subsystem software can be made sufficiently reliable to support the 10(-10)/hour survivability goal.

7.2 Trade-Off Parameters

The principal trade-off criteria will emphasize fault-tolerance, periodic maintenance and expansion capabilities.

1) Fault-Tolerance Capability

The advance flight control system must meet the 10-(-10)/hour survivability goal. The susceptibility to system failure is the principal measure of the candidates' qualifications. The causes of system failure are:

Exhaustion of Resources

The candidate must provide a sufficient reserve of resources to replace failed elements. Failures must be correctly identified and isolated to avoid disengagement of non-failed components. The resources or

redundancy level of the conventional system are fixed and cannot be expanded if the necessity should arise. Moreover, since resources are dedicated, there is no access to resources outside of the flight control system. To overcome these deficiencies, the conventional system must resort to indirect data obtained by analytical redundancy techniques.

In the conventional, centralized system, components tend to be large and complex with correspondingly large failure rates with little capability for cross-strapping. The distributed system, by using smaller and more reliable elements, has a greater reliability potential than its centralized counterpart. To illustrate, consider a quad set of processors such that loss of 3 or 4 processors in a single flight of one hour results in loss of system. The probability of this event is

$$S = 4\lambda^3 + \lambda^4$$

where λ = failure rate/hour of a single processor.

In a distributed system with m, quad sets of microprocessors, the corresponding probability is

$$S(d) = m\,(4\lambda_d^3 + \lambda_d^4)$$

where λ_d = failure rate/hour of a single microprocessors,

assuming that each quad set is flight critical and there is no cross-strapping.

Typically

λ = 300 x 10(-6) for a conventional flight control computer.

If we conjecture (see section on "Parallel Processing" for a more realistic estimate) that

λ_d = 50 x 10(-6) for a microprocessor

then

$$Sd/S = 220m.$$

Thus, the distributed system can employ 220 quad sets before it exceeds the unreliability of the centralized system, even without resorting to its inherent cross-strapping capability. Of course, the example is an oversimplification but it illustrates the point.

Software Errors

A redundant system that employs identical software in its redundant processors is susceptible to loss of function due to a single software error. In as much as software errors are a strong function of discipline and procedures, which are independent of architecture, it is difficult to assess an architecture's potential for minimizing these errors. We can only conjecture that the proposed partition of software into smaller and physically independent modules will tend to simplify software and software validation and make the total system less vulnerable.

Single-Point Faults

Single-point faults are similar to software errors in that a single fault can result in loss of redundant elements. Generic hardware faults are in this category. The principal sources of single-point faults in the proposed architecture are the bus controller and 1553B remote terminals (i.e., the babbling terminal). Since a single-point fault can cause loss of a critical subsystem there is little to choose between a conventional and advanced architecture from the standpoint of these faults.

Inability to Detect and Isolate Faults

In order to keep redundancy at manageable levels, fault detection and isolation are essential in both the conventional and advanced systems. Faults tend to more visible and isolatable in the advanced system. A novel feature of the proposed architecture is the expanded role of the bus controller, i.e.,

- monitoring redundant variables transmitted over the local network;
- maintaining failure status;
- reconfiguration management.

The bus structure provides the bus controller with access to all subsystems. A a consequence, the bus controller is ideally situated to perform monitoring and reconfiguration.

Almost Simultaneous Faults

These are faults which occur in close time proximity, the second occurring before the first has been detected and isolated. These faults can have a significant impact on systems with survivability goals of the order of 10(-10)/hour. As an illustration of this effect Table 8 gives the probability of a single component failure in 10, 50, and 100 milliseconds as a function of the failure rate of the component. In a system of triplex processors, for example, with

- frame time = 100 milliseconds
- failure rate of a single processor = 300 x 10(-6)/hour

the probability of a second failure occurring within a frame of the first failure is

2 x 83.3 x 10(-10).

As a consequence, a candidate system must be capable of tolerating almost simultaneous faults either through the use of more reliable components or higher levels of redundancey. By distributing tasks over smaller and more reliable processors and by accommodating greater redundancy, the advanced architecture meets these requirements.

Latent Faults

Latent faults are temporarily dormant but could become active in response to a single source of excitation. Recent studies, conducted by Bendix under contract to NASA Langley Research Center (Ref. 12), indicate that a significant proporation of faults are latent in a comparison-monitored system. In an emulation of a high performance inner-loop flight control system, consisting of 2200 assembly language instructions, approximately 40% of all gate-level faults remained undetected after 8 frames of computations. Unless special means are provided for their detection, latent faults will accumulate in redundant channels and could eventually be triggered by a single excitation. The result would be a rapid and unanticipated exhaustion of components. The effect on survivability has yet to be determined: this is one of the objectives of the CARE III reliability model.

The advanced system, by distributing tasks among independent, smaller and more reliable elements

- minimizes the occurrence of latent faults in redundant, similar elements and
- localizes their effects, if they should occur.

Providing extra redundancy does not solve the latent fault problem. Eventually, latent faults must be detected and removed from the system. The solution is to apply an extensive system self-test, periodically, with the period and coverage determined by the predicted accumulation of latent faults and the degree by which they reduce survivability.

Intermittent Faults

These faults are the result of borderline design defects or external disturbances. The frequency of intermittent faults has not been determined but estimates have placed the rate at an order of magnitude greater than the failure rate of a typical flight control channel. Intermittent faults could result in premature exhaustion of components or confuse fault detection and isolation strategies. The solution is to insist that a fault persist for several frames before the affected unit is disengaged from the system. However, because of the possible occurrence of a second fault in the interim, the system must provide the necessary, additional redundancy to tolerate multiple faults. The flexibility to add redundancy and to reconfigure as the situation demands, is a key feature of the proposed architecture.

2) Periodic Maintenance Capability

One of the potential economies of the advanced architecture is an extended maintenance period. One of the benefits of the proposed architecture is that it can incorporate any number of spare subsystems by simply connecting them to a local network. The procedure for bringing a spare on-line and integrating its functions is dependent upon the subsystem configuration and will vary for different subsystems. In an case, the procedure is considered to be the responsibility of each subsystem; the bus controller will participate only to the extent of rearranging the data transmission.

A detailed analysis of spares requirements is given in Appendix B. The results and conclusions are summarized here.

Maintenance Stratigies

1. Scheduled, powered spares.

2. Scheduled, unpowered spares.

3. Unscheduled, powered spares.

4. Unscheduled, unpowered spares.

In scheduled maintenance, maintenance is performed at prescribed times whereas, in unscheduled maintenance, maintenance is only performed as required to maintain system integrity.

Conclusions

1. Maintenance requirements are extremely sensitive to the failure rate of the elemental units (LRU's) for both scheduled and unscheduled maintenance.

2. The number of spares required for a 1500 hour (biannual) scheduled maintenance period are given in Table 9 for several component failure rates. From the table it can be seen that 15 powered spares are required when the component failure rate is 300 x 10(-6)/hour whereas only 4 are required when the failure rate is 50 x 10(-6)/hour.

3. The number of spares required to insure that the probability of unscheduled maintenance action in 1500 hours does not exceed 1/10 is given in Table 10 for several component failure rates. The table also gives the mean time between maintenance actions. Comparing Tables 9 and 10 it can be seen that if a one in ten probability of a maintenance action is acceptable, unscheduled maintenance can achieve very respectable average maintenance periods with a modest complement of spares.

4. The cost of spares in scheduled maintenance can be prohibitive especially for subsystems with component failure rates of the order of 300 x 10(-6)/hour (e.g., of a typical CPU, including I/O).

5. From the standpoint of spares required it is preferable to employ unscheduled maintenance and distribute the system among many but more reliable components. The benefit of distribution is further enhanced, if a single spare can be used as a replacement for any one of several dissimilar components.

3) Expansion/Modification Capability

The ability of the proposed architecture to expand its functions has been described, repeatedly, in previous sections. In summary, this capability is the result of the structure of the local bus network, the role of the bus controller as reconfiguration manager and the use of parallel application processing. It is difficult to envision how a conventional architecture could provide the equivalent capability.

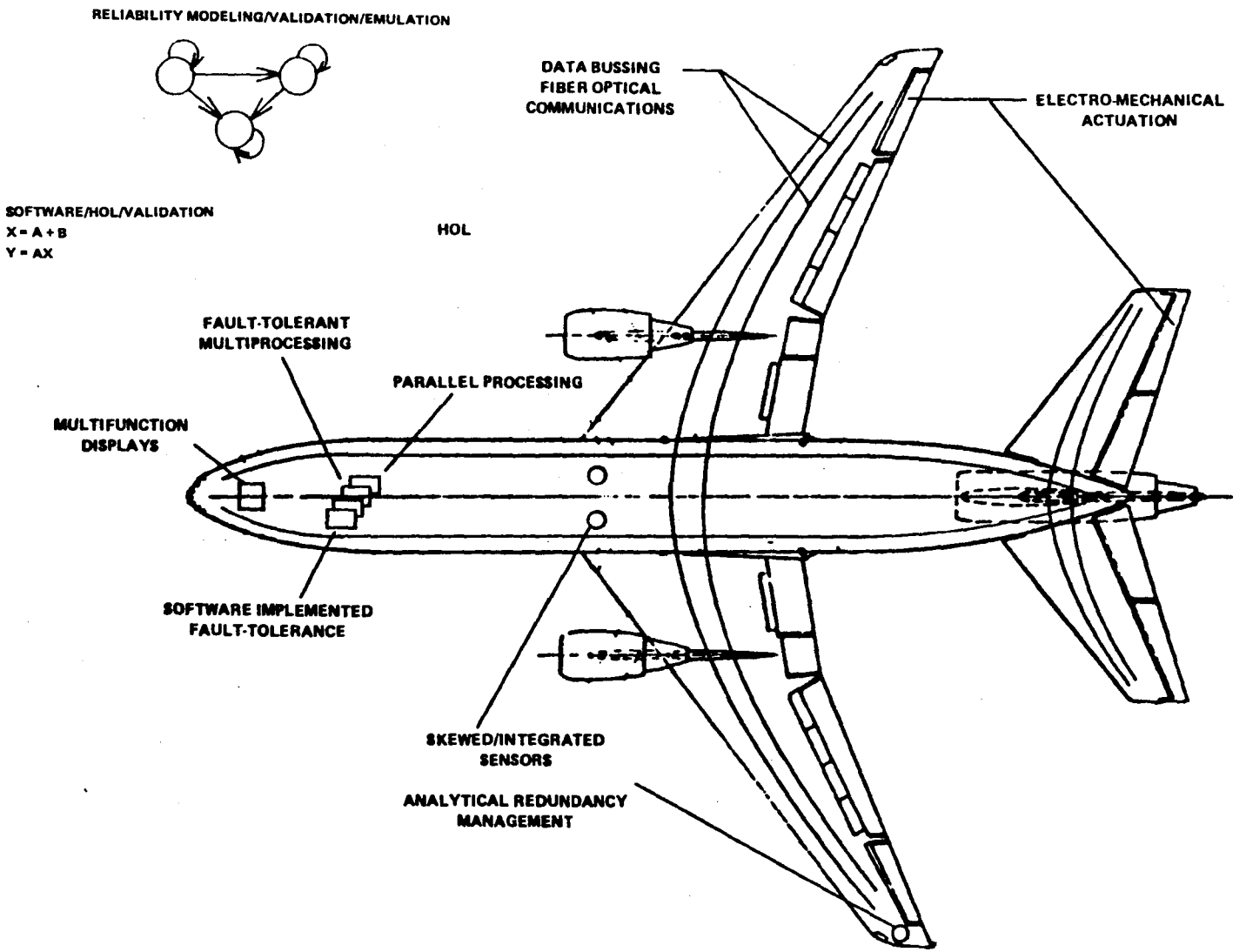


Figure 51 New Technologies

TABLE 7

NEW TECHNOLOGIES

TECHNOLOGY	SUPPORTING TECHNOLOGY
1. HOL POTENTIAL BENEFITS • VALIDATED COMPILER • DISCIPLINED PROGRAMMING • IMPROVED VISIBILITY • SIMPLIFIED VALIDATION	1. STANDARDIZED PROCESSOR E.G. 1750A
2. RELIABILITY MODELING/VALIDATION • IMPROVED SAFETY • AID TO SYSTEM DESIGN • COVERAGE REQUIREMENTS • SENSITIVITY ANALYSIS	2A. CARE II, CARE III, MARKOV MODELS 2B. EMULATION
3. PARALLEL PROCESSING • IMPROVED REAL-TIME • SIMPLIFIED SOFTWARE • SIMPLIFIED VALIDATION • IMPROVED RELIABILITY • GROWTH CAPABILITY • IMPROVED SOFTWARE MAINTENANCE	3. LSI TECHNOLOGY
4. FAULT-TOLERANT MULTIPROCESSING • HIGH RELIABILITY • IMPROVED MAINTENANCE	4a. HOL 4b. SOFTWARE VALIDATION 4c. RELIABILITY MODELING 4d. ANALYTICAL REDUNDANCY MGMT 4e. SKEWED/INTEGRATED SENSORS 4f. BUS NETWORKS 4g. SELF-TEST

TABLE 7

NEW TECHNOLOGIES (CONT'D)

TECHNOLOGY	SUPPORTING TECHNOLOGY
5. SOFTWARE IMPLEMENTED FAULT-TOLERANCE • REDUCED HARDWARE, i.e. ECONOMY • FLEXIBILITY • IMPROVED CONTROL • IMPROVED FAULT DETECTION, ISOLATION	5a. FAULT-TOLERANT MULTIPROCESSING 5b. SOFTWARE VALIDATION 5c. EMULATION 5d. ANALYTICAL REDUNDANCY MGMT 5e. SKEWED/INTEGRATED SENSORS 5f. BUS NETWORK
6. MULTIPLEXED DATA BUSSING • ECONOMY (e.g. Weight Reduction) • IMPROVED CONTROL • RECONFIGURATION CAPABILITY • IMPROVED VISIBILITY • CENTRAL MONITORING	6a. STANDARD INTERFACE HARDWARE 6b. STANDARD PROTOCOL 6c. FIBER OPTICS 6d. RELIABLE BUS CONTROL
7. SOFTWARE/SOFTWARE VALIDATION • ECONOMY • RELIABILITY • VISIBILITY	7a. IMRPOVED DISCIPLINE 7b. PARALLEL PROCESSING 7c. HOL 7d. STANDARD PROCESSOR
8. ANALYTICAL REDUNDANCY MGMT • ECONOMY • IMPROVED FAILURE DETECTION	8. BUS NETWORK, i.e. ACCESSIBILITY OF RESOURCES
9. SKEWED/INTEGRATED SENSORS • ECONOMY • RELIABILITY	
10. ELECTRO-MECHANICAL ACTUATION • ECONOMY	10. IMPROVEMENT IN STATE-OF-THE-ART

TABLE 7

NEW TECHNOLOGIES (CONT'D)

TECHNOLOGY	SUPPORTING TECHNOLOGY
11. MULTIFUNCTION DISPLAY • ECONOMY • IMPROVED VISIBILITY	11. STANDARDS
12. FIBER OPTICAL COMMUNICATIONS • IMPROVED EMI • ECONOMY • GREATER BANDWIDTH	12a. BUS NETWORK 12b. IMPROVEMENTS IN STATE-OF-THE-ART

TABLE 8

CONDITIONAL PROBABILITY OF A SECOND FAILURE GIVEN FIRST FAILURE

Failure Rate (per hour)	Frame Time (milliseconds) 10	50	100
50 x 10(-6)	1.39 x 10(-10)	6.94 x 10(-10)	13.88 x 10(-10)
100 x 10(-6)	2.78 x 10(-10)	13.9 x 10(-10)	27.8 x 10(-10)
200 x 10(-6)	5.56 x 10(-10)	27.8 x 10(-10)	55.6 x 10(-10)
300 x 10(-6)	8.33 x 10(-10)	41.7 x 10(-10)	83.3 x 10(-10)
500 x 10(-6)	13.9 x 10(-10)	69.4 x 10(-10)	138.8 x 10(-10)
1000 x 10(-6)	27.8 x 10(-10)	138.9 x 10(-10)	277.8 x 10(-10)

TABLE 9

NUMBER/SPARES REQUIRED FOR A SCHEDULED MAINTENANCE PERIOD = 1,500 HOURS

Failure Rate	Number of Spares Required	
	Powered Spares	Unpowered Spares
300 x 10(-6)/	15	10
100 x 10(-6)/	6	6
50 x 10(-6)/	4	4

TABLE 10

NUMBER OF SPARES REQUIRED FOR THE PROBABILITY OF A MAINTENANCE ACTION IN 1,500 HOURS NOT TO EXCEED 1/10

Failure Rate (per hour)	Number of Spares Required	
	Powered Spares	Unpowered Spares
300 x 10(-6)/hr	6 (2,819)	4 (3,333)
100 x 10(-6)/hr	3 (5,095)	3 (7,500)
50 x 10(-6)/hr	2 (7,333)	2 (10,000)

( ) = Mean time between maintenance actions (Hours)

8.0 VALIDATION AND DEMONSTRATION METHODS

A demonstration of 10 -10/hour survivabiity by observing the total system either in simulation or in the field is clearly impracticable. The number of statistical fault injection experiments required would be of the order of 10(10) for a credible assessment. As a consequence, survivability will be demonstrated, indirectly, by estimating reliability-related data associated with single failure events and combining the results, analytically, to obtain system survivability. By focussing attention on single failure events, with relatively large probabilities of occurrence, the number of samples required to estimate a statistic through laboratory or flight experience is reduced to the point where it becomes a practicable undertaking.

8.1 Analytical Methods

The proposed approach requires

1. a reliability model which identifies and incorporates all of the essential parameters affecting survivability and

2. estimates of these parameter values

The reliability model will be used to conduct studies to determine the sensitivity of selected parameters to survivability. Critical ranges of these parameters will be identified and laboratory and flight experiments will be used to estimate them.

Reliability Model

It may be said that a flight control system design is an implicit implementation of the designer's reliability model. The levels of redundancy, monitoring and reconfiguration strategies are determined by this model. An explicit reliability model is an essential ingredient of the design process because it forces the identification and quantification of key reliability parameters and provides the basis for design trade-offs.

In conventional military systems, with reliability goals of the order of 10 -7/hour, experience has shown that a simple reliability model will suffice. This model generally assumes that there are no failures in the system at the start of each flight; that latent faults either do not exist or their effects can be ignored. Effectively, the model is simple because it is relatively easy to identify failure events that are commensurate with the 10 -7/hour goal.

In advanced and critical flight systems however, the reliability model must include failure events that were ignored in the simple model. Without experience as a guide it is by no means clear what reliability parameters should be included. What is required is a reliability model sufficiently comprehensive to include a variety of such parameters and, at the same time, produce results accurately and in a reasonable amount of time. With such a model it would be possible initially to perform sensitivity studies on likely parameter candidates to ascertain their effect on overall systems survivability. As a result of this study key reliability parameters would be identified and the designers would be alerted to their importance in the system design.

For a comprehensive survey of reliability models the reader is referred to (ref. 18). Care III appears to be the most powerful of all the models reviewed. It is currently undergoing test trials at Boeing, under contract to Nasa Langley Research Center. Information available indicates that the development is far enough along that the major technical problems have been overcome and the model may be available for restricted use in mid 1982.

Care III (Computer-Aided Reliability Estimation) is an outgrowth of an earlier model called Care II. A Markov chain is an inherent feature of both models. The system state at any given time is characterized by all those parmeters needed t determine both the likelihood that it will experience a fault and the probability that it will successfully detect, isolate and recover from the fault. These various system states are then interrelated through a set of transition functions representing the rate at which the system state changes from any given state to any other state. A single channel (or computer, or processor, etc) is divided into stages, e.g., processor, memory and bus. System states are obtained by combining all stages of all redundant elements in every possible combination and for every possible fault mode. A fault mode is defined by all those parameters needed to determine the systems vulnerability to subsequent faults, e.g., detected, undetected, latent, intermittent, etc. The number os such states can be extremely large. One of the advantages of Care III is its ability to significantly reduce the number of possible states by, effectively, analyzing the fault-occurrence events separately from the fault-handling processes and later combining these in the overall model.

In summary, Care III can be used to model

- systems with large numbers of states
- time-dependent transition probabilities

- time-from-entry-into-state transition probabilities
- up to 40 stages
- latent, intermittent, permanent and transient faults
- failure detection coverage
- reconfiguration time
- effects of spares, powered and unpowered.

8.2 Laboratory Testing

Laboratory and flight methods will be used to:

- establish reliability data associated with single failure events
- confirm and validate assumptions and conclusions of the reliability model.

Flight tests will be employed to validate laboratory results by duplicating specific data points (e.g. flight condition, failures, etc) in actual flight environments.

Laboratory testing will consist of:

1. fault injection experiments using gates and pin-level emulations of major system components;
2. closed-loop testing using actual and simulated hardware.

Emulation

One of the problems of using a refined reliability model such as Care III is the unavailability of fault modeling data. While themodel can be used to perform sensitivity studies, in the final analysis actual values are required. During the past several years Bendix Flight Systems Division, under contract NAS1-15946 to Nasa Langley Research Center, has used a gate-level emulation of the Bendix BDX-930 CPU as the basis for a series of fault injection experiments to determine:

- the applicability of gate-level emulation to fault analysis of digital systems;
- the time required to detect faults in a comparison - monitored system;
- fault detection coverage of a typical self-test program.

The results (ref. 12) of the study demonstrated that emulstion was a practical and viable approach to FMEA analysis and could be used as a tool to obtain reliability data such as:

- time to detect faults (e.g. fault latency)
- proportion of latent faults
- self-test and BIT coverage
- ability to isolate faults
- effects of single point faults
- effects of almost-simultaneous faults
- proportion of faults affecting control surfaces
- effects of intermittent and transient faults
- vulnerability of 1553 B to babbling

It is proposed to emulate, at the gate-level, the advanced architecture including:

- 1553 B local network, a remote terminal, the bus controller terminal and associated bus interface hardware;
- an application processor subsystem such as SIFT.

Experiments will consist of injecting faults and observing the resultant system response. If it is assumed that the bus controller and application processors are comprised of BDX-930 computers then the cost of the emulation experiments can be greatly reduced since the BDX-930 gate-level emulation already exists.

It is proposed to use the NASA Airlab Test Facility for performing the emulation, provided that the facility can be made available to this program. The facility can be used to demonstrate both normal performance and performance when subjected to failures. In addition, ongoing experiments would be conducted to update the system by the addition or substitution of new processors/technologies. As an example, the use of fiber optic busses could be demonstrated.

In addition to obtaining generic reliability data the facility could be used to evaluate:

- bus loading
- bus error rate
- throughput of parallel processors
- time delays (transport lag in the parallel processor and the 1553 B bus system)
- asynchronous performance feasibility
- reconfiguration time
- nuisance alarm susceptability
- noise effects

Appendix C describes a closed loop test facility that is available at Bendix Flight Systems Division. This facility can easily be modified to the requirements of this program. Among the modifications being considered at this time, for example, is tying this facility to a more powerful general purpose digital computer (VAX 11/780), available at Bendix and, consequently, to the entire Bendix VAX network. This will multiply the capacity of the facility.

The facility would be used to verify and validate the software on a system basis, as well as to verify that aircraft performance is acceptable over the entire flight regime and for all system modes. In other words, it will check out the control laws as well as their software implementation. Fault injection experiments can be performed, down to the component level on the hardware to verify that the fault detection, isolation, and reconfiguration algorithms have been correctly programmed.

Figure 52 is a graphic representation of the interactions of the various laboratory software tests. It is assumed that all programs will be written in a higher order language, such as Fortran or Jovial (J-73). For example, a Jovial J-73 compiler is available already for the Z-8000 microprocessor. It is expected that in the time span of this program, suitable compilers will be available for any microprocessor that one would wish to use.

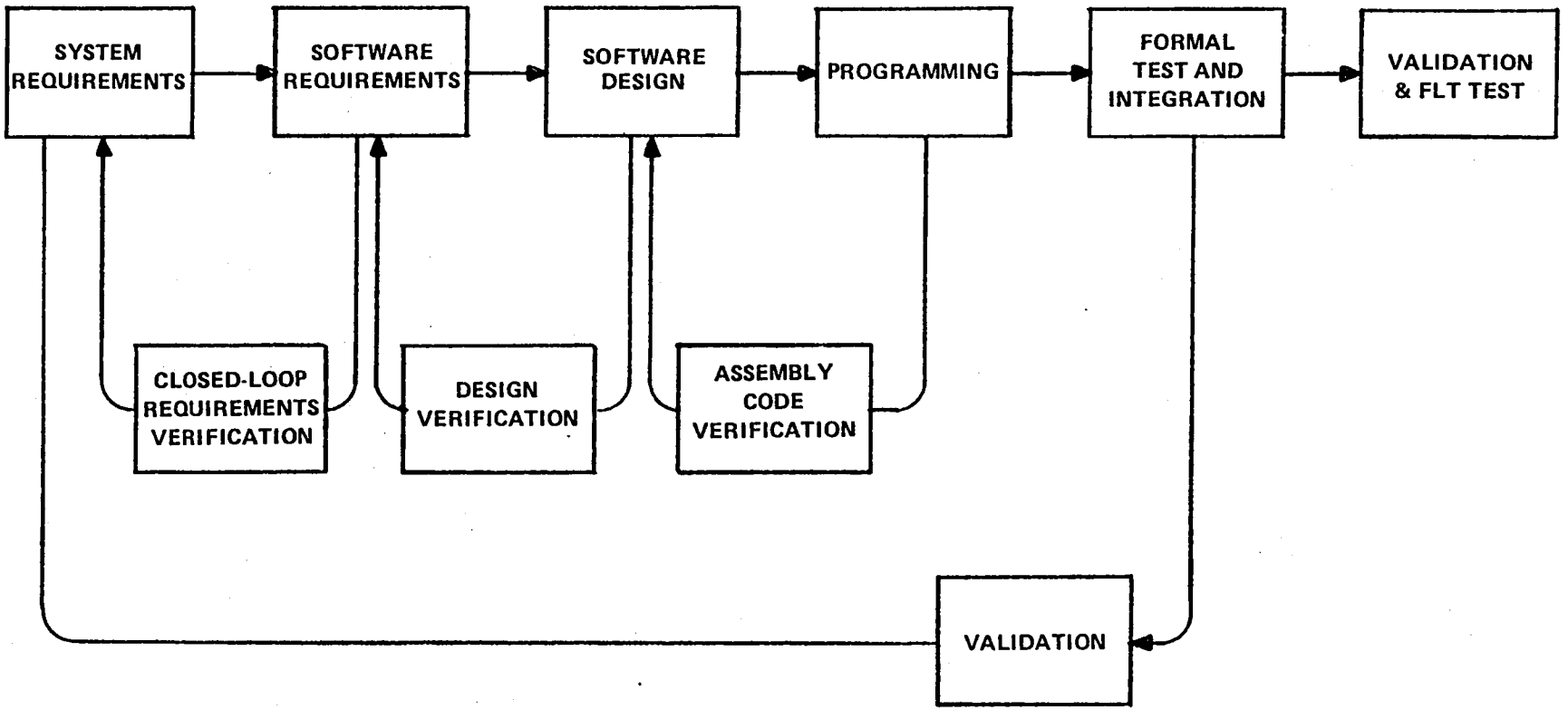


Figure 52 Software Test Summary

9.0 TEST-BED AIRCRAFT

9.1 Introduction

Selection of the test-bed aircraft is a highly subjective task. Three major factors surface in the evaluation: (1) availability to NASA-Dryden, (2) the extent of the modifications required to the aircraft, and (3) the configuration of the aircraft with respect to desirable test-bed characteristics.

The major emphasis is given to availability to NASA since a vehicle is not a real candidate unless it is possible to obtain it. The other factors are:

Modifications:

- Irreversible Control System
- Ease of Control System Modifications
- Airline Demonstration Suitability

Desirable Characteristics:

- Safety
- Two-man Crew
- Equipment Installation Space
- Passenger Capability (Cabin)

The primary question to be asked of a flight demonstrator vehicle is "does the system do the job," i.e. performance, demonstrability, and safety.

It is considered basically impossible to demonstrate reliability to any reasonable extent in a single flight demonstrator vehicle. The basic limitation is time available. One year has a total of 8760 hours possible demonstration time available. Thus, even 10 years of continuous demonstration only gives 87,600 hours available at most. Practically, only a fraction of that time is available. Thus, it is not possible, in a practical sense, to verify reliability goals on the order of 10^{-9} or 10^{-10} hours MTBF on a single test article.

A fleet demonstration with enough aircraft and enough hours could provide statistically valid reliability data. It is required, however, that any system which is a candidate for flight demonstration in a fleet environment, either commercial or military, be adequately tested before

introduction into the fleet. Adequate testing of the technology before fleet introduction need not be on a similar vehicle. It is only necessary that the technology be compatible.

An additional consideration is that advanced flight control configuration concepts are applicable to both low and high performance vehicles. In the area of maneuvering requirements, the actuator specifications are significantly more challenging in a high performance vehicle than in a low performance vehicle. Thus, while there may be areas of overlap between high and low performance configurations, there are enough significant differences to warrant consideration of two separate test-beds, one low performance and one high performance vehicle, in order to fully explore the realm of Advanced Flight Control Systems.

Gulfstream STA Test-Bed Potential

One possible test-bed aircraft for Advanced Flight Control System flight evaluation program is the NASA STA. The STA airframes are subjected to a severe fatigue environment and they are closely monitored and inspected for structural integrity. Thus, a possible source would be a fatigue damaged STA in the NASA inventory. An aircraft of this type could be repaired and put into service as an Advanced Flight Control System test-bed.

Another possible source for a Gulfstream test-bed would be an airframe procured by NASA in anticipation of need of a STA requirement. This would be based on future STA requirements in the early 1990's. On this basis NASA would procure a Gulfstream II in 1985 in anticipation of need for conversion to a STA article and delivery in the early 1990's. Once in the NASA inventory it could be bailed to the Advanced Flight Control System study for interim use as a test-bed.

There are several advantages to NASA with this approach. After procurement by NASA the aircraft would be under NASA control and its flight time and environment would be precisely known. The STA airframe modifications could be made at the time of the FBW changes, thus equipping the aircraft with the major STA elements of DLC, SFC and reverse thrust. The use of the aircraft for FBW tests would not put high time or stress on the airframe while it would keep the airframe in an airworthiness status.

9.2 Advanced Flight Control System Test-Bed Summary Description

The Gulfstream II STA aircraft offers several advantages as a candidate for the Advanced Flight Control System Test-Bed (Figure 53).

Primarily it is a mini-commercial type vehicle, having an airways capability. It has a two man crew and the 1400 cu. ft. of cabin space with 5600 lb. payload potential provide it with very adequate capability for avionics equipment installation and an engineering test station.

The cockpit instrument panel easily accommodates six CRT displays, two for each pilot as a vertical and horizontal display and two in the center panel for the advisory and warning tasks, Figure 54. These CRT's are in addition to the basic vertical engine instruments in the center panel and leave adequate space for conventional three inch instruments on either side of each pilot's CRT displays.

The basic STA is equipped with a LM type hand controller at the pilot station and a conventional Gulfstream II control wheel and column at the co-pilot station. This installation is maintained for the baseline FBW configuration since it offers the capability to evaluate both types of controllers in a test environment. Retaining the control wheel and column requires the installation of a feel device for proper operation. Alternately, the cockpit could be configured with dual FBW hand controllers.

The cabin space is very adequate for installation of each channel of the multi-channel avionics system in a separate pallet, Figure 55. Each channel is thus physically isolated from each other and, installed in the seat tracks, inflicts no scar or structural change to the aircraft. The pallet provides monitor and test panel capabilities in order to assess operation of the system to whatever level is necessary. In addition, the pallet concept allows each channel to be fully inter-wired and tested outside of the aircraft which significantly reduces the amount of aircraft time required for detailed sub-system checkouts. The electrical connections on the pallet are to the various airframe systems and interconnections to the other pallets.

The STA is equipped with a Hewlett-Packard tape recorder which records 273 words provided by the digital simulation system every 50 milliseconds (the basic computer cycle). In the STA many of these words pertain to the simulation model and simulation process. Thus interfacing this recorder with the FBW avionics system through the engineers' station provides a fairly comprehensive data recording system.

The STA is equipped with fast acting Direct Lift Control (DLC) and Side Force Control (SFC) systems. The primary use of the control surfaces in STA simulation is to provide the simulation pilot with the rotational forces he feels while controlling a vehicle much larger than the Gulfstream II. This capability is implemented in the STA with two DLC and two SFC electro-hydraulic actuators.

One application of the DLC surfaces could be toward enhancement of approach and glideslope control. This capability exists on some current aircraft and is certainly a candidate for future aircraft. The FBW STA Gulfstream would have this capability. While it is not within the scope of the Advanced FCS study, these SFC and DLC features would provide the aircraft with the capability to provide the simulation fidelity required to evaluate a FBW SST or other large airframe. If the FBW Gulfstream does not utilize these features, the DLC actuators can be replaced with a bar linkage and the SFC's can be locked in position or removed from the airframe.

The FBW modifications to the control system involve removal of the aircraft cable and trim systems and the addition of electrically controlled actuators to provide inputs to the surface controls. Two dual electrohydraulic actuators in each primary control axis are baselined for this purpose. A third hydraulic system, electrically powered by the Auxiliary Power Unit (APU), provides the power to one of the actuators. The basic flight and combined hydraulic systems provide dual power to the other actuator. This configuration gives a two fail-op capability and also provides flight control with both engines out.

The electrical system is to be modified to provide uninterruptible power and to add a third system with in-flight APU operation. An increase in the battery size will provide 30 minute fail-safe operation in this mode.

While the primary safety considerations in this aircraft are satisfied with redundancy, the ability for a rapid egress provides a certain level of security in the crew. The Gulfstream flight test programs have utilized a kick-out baggage door with an air deflector as the basic exit area. With the high tail and forward engines this exit provides a clear area for separation from the aircraft. It has been used with cargo drops. The means used to get to the door have been a powered cable tow or a hand rope. These techniques have been satisfactory to the crews.

an additional level of safety could be provided, at least for the initial flights, by retaining the primary cable control systems. This would result in a configuration similar to, but slightly more complex than, the baseline FBW configuration. The primary interface between the cable system and FBW actuators would be with a shift mechanism at the sector. Detail design of this sector would allow summation of the cable and actuator inputs with the shift activated. The actuators would require a positive means for hydraulic disablement and by-pass should direct manual control by required. While this configuration is mentioned here as a possibility it is not recommended. It would only be considered further if the need for a back-up system arose.

A fully operational and configured iron bird was used for Gulfstream II and STA flight control system development. This iron bird is in storage at Grumman and available for the Advanced Flight Control program. Its use for design confirmation and test of the entire system is considered mandatory.

The iron bird tests on the basic control system will address the capability of the control system in terms of performance, strength, stability, failure modes, etc. Confirmation of some of the test results on the aircraft would be required. The iron bird would also be electrically integrated with the avionics system for system development. It would be further integrated with a full aerodynamic airframe simulation for closed loop "simulated in-flight testing". While avionics integration can be accomplished on the aircraft during installation, this testing would be, by necessity, later in the program.

Additional tests required on the aircraft include a build-up functional test of the hydraulic and electrical systems, the control systems and the avionics systems. These would be followed with very thorough GVS (Ground Vibration Survey) and EMC (Electro-Magnetic Compatibility) test programs.

Following these tests, a flight readiness test (FRT) and flight readiness review (FRR) will clear the aircraft for flight.

Flight tests at Grumman are airworthiness tests designed to verify the basic integrity and operation of the aircraft. Following airworthiness acceptance the formal test program will begin. While it is difficult to demonstrate reliability and maintainability with a single test article in a limited amount of time, it is most certainly appropriate to demonstrate the features which are designed into the system to provide these qualities.

The key to the reliability feature is fault tolerance, the ability of the system to continue satisfactory operation after several faults. Thus, the test program must demonstrate the extensive fault tolerant capability of the system. Integrated with this feature is fault detection and isolation. Proper fault management will retain the failure records for maintenance action, thus allowing this aspect of maintainability to be addressed. Detail hardware and installation dependent maintainability items could not be evaluated with a test configured article.

Overall, the Gulfstream provides an excellent test-bed to perform Advanced Flight Control System evaluations for the baseline program and it has the inherent capability for advanced programs with in-flight simulation.

Appendix H describes the STA and provides details of the basic modifications to be performed on the aircraft, and basic data concerning the following systems.

Crew Systems and Equipment
Flight Control Systems
Hydraulic Power System
Electrical Power System
Auxiliary Power Unit
Air Data System
Guidance, Navigation and Control Systems

9.3 Airworthiness Flight Test Program

Following the satisfactory completion of factory acceptance tests but prior to the first flight of the aircraft, a Flight Readiness Test (FRT) and Flight Readiness Review (FRR) will be conducted. The FRT is an indepth functional checkout of the integrated aircraft systems with results checked against pre-determined standards. The FRR provides an objective Grumman and customer review of the disposition of any and all failures and anomalies uncovered during the vehicle's acceptance tests and FRT to insure that the aircraft is in fact ready for first flight.

In order to assure that the vehicle modifications and the new flight control system (FCS) are working as designed and can be safely operated within the operating flight, the contractor will perform an airworthiness test program. The objectives of this program are as follows:

- Demonstrate a safe operating envelope for NASA
- Demonstrate satisfactory handling qualities of the new FCS/airframe combination
- Validate the functional operation of the FCS and the Engineers Station
- Demonstrate satisfactory failure mode operation
- Flight qualify the APU system for 3rd system hydraulic and electric power
- Evaluate the functional operation of all subsystems
- Demonstrate satisfactory operation of the cockpit displays

Specific maneuvers will be flown throughout the recommended flight, e.g. and weight envelope. Static and dynamic maneuvers will be performed to define the airframe and FCS characteristics. These maneuvers will measure, validate and assess the following items:

- Static and dynamic airframe stability
- SAS operation
- Trimmability
- Control harmony
- FCS performance
- FCS stability, lag and transient characteristics
- FCS management
- Landing and takeoff characteristics
- Closed loop handling qualities
- Stall prevention
- Control force breakout and gradient characteristics
- Cockpit displays
- Autopilot performance

Flight verification of all FCS functions will be conducted by the crew including failure mode operation. Concurrently, operation of all systems including subsystems will be functionally evaluated.

An onboard tape recorder will record pertinent parameters for post flight analysis. Critical parameters will be telemetered to the GAC ATS for real time monitoring and analysis. All flight operations will be conducted from the contractor's Calverton facility.

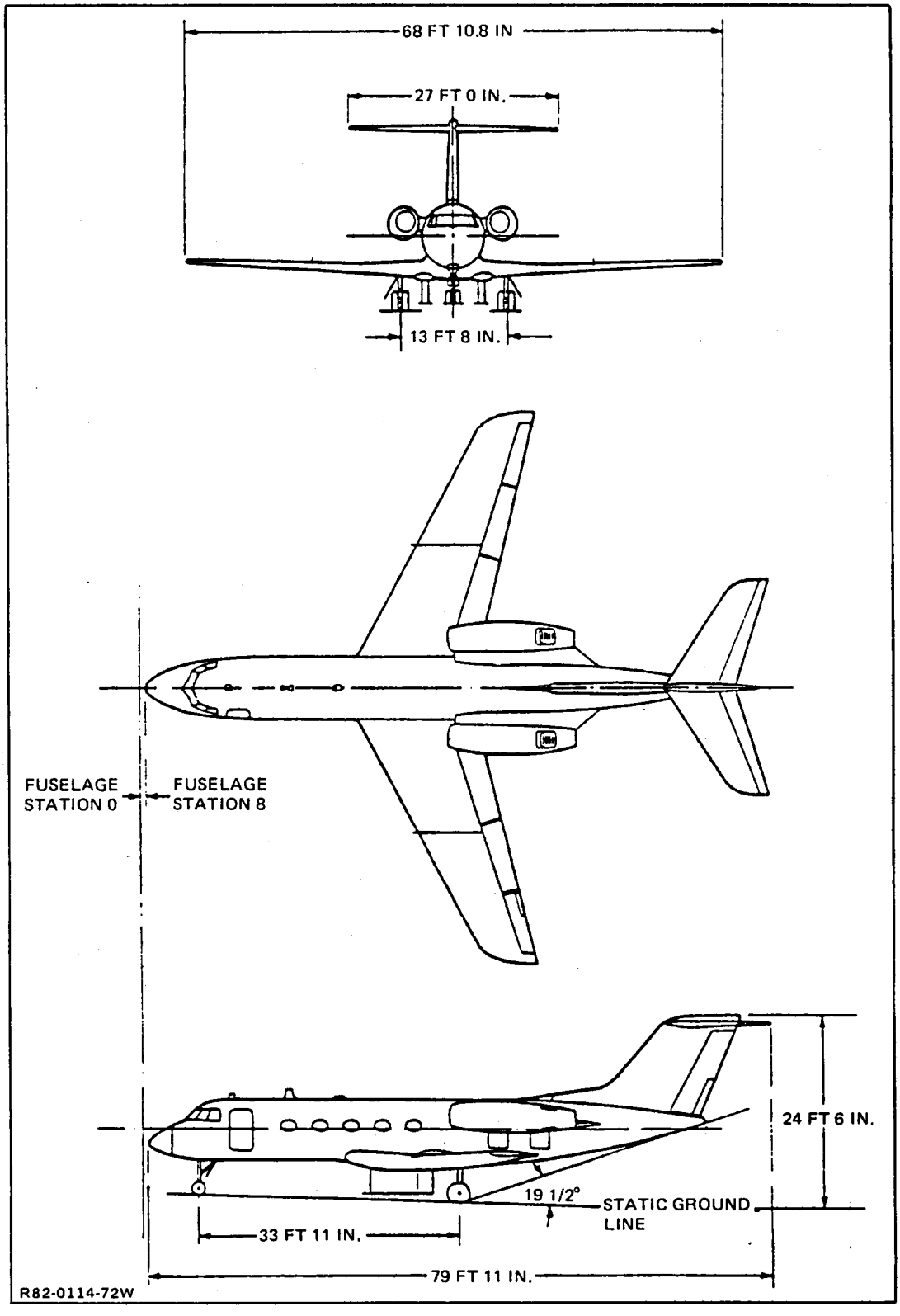


Figure 53 Shuttle Training Aircraft General Dimensions

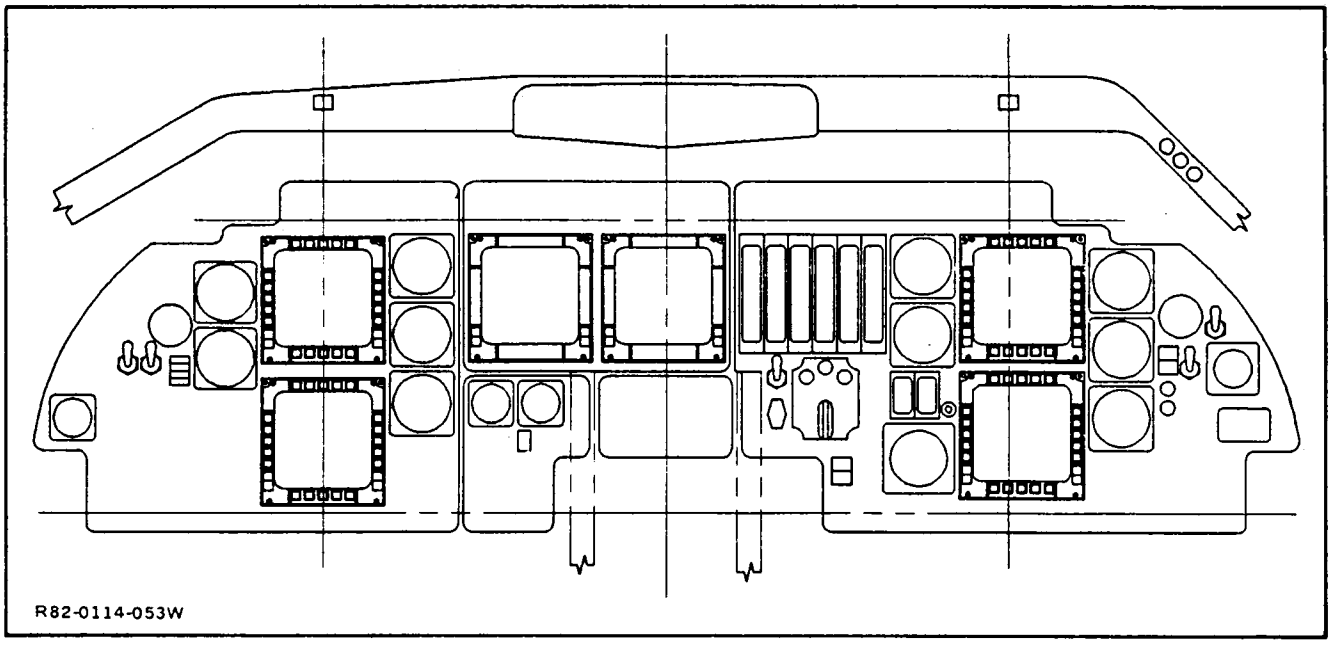


Figure 54 FBW Gulfstream Instrument Panel Arrangement

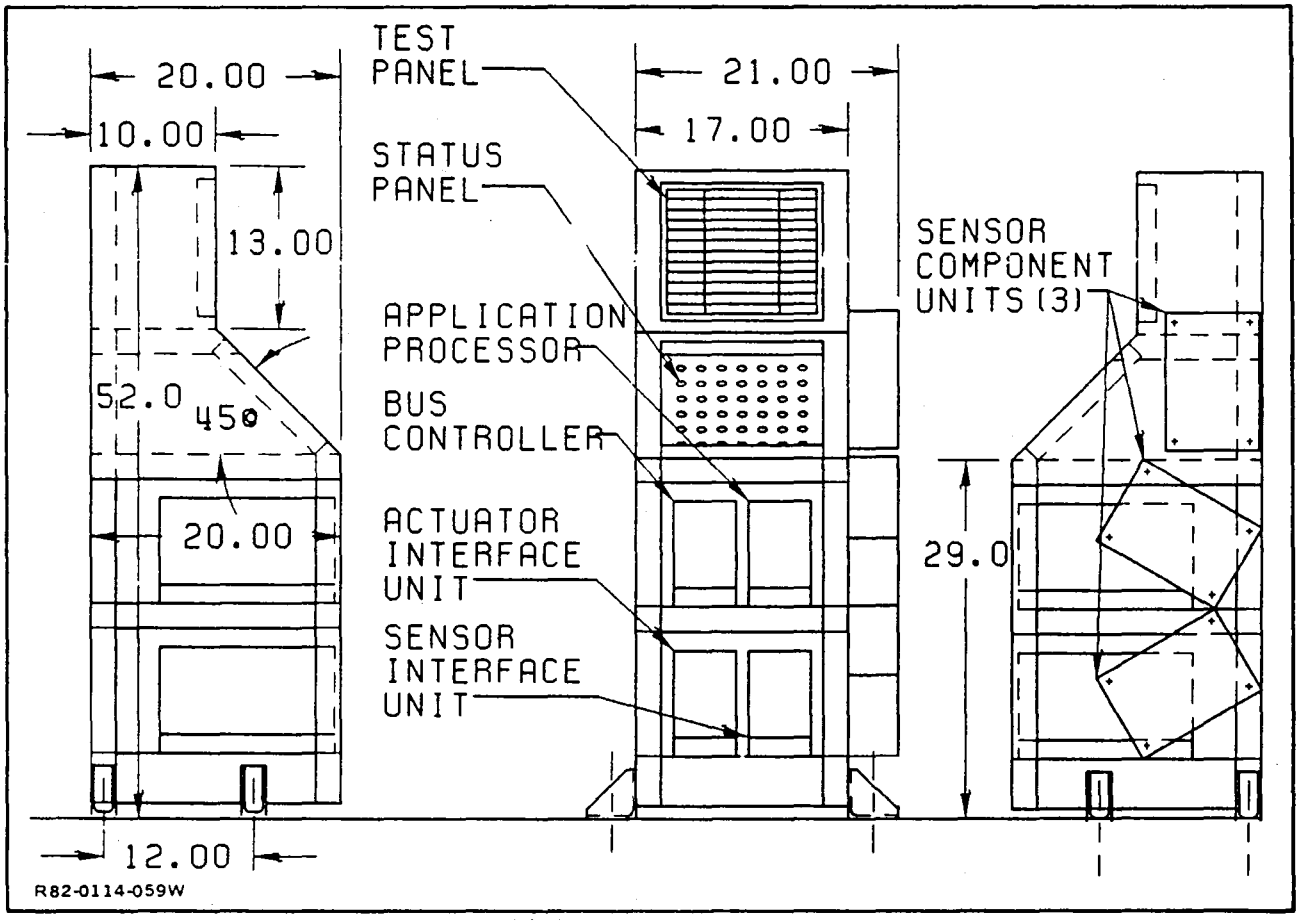


Figure 55 Fly-by-Wire Pallet

10.0 REFERENCES

(1) Weinstock, C. B., Goldberg, J., "SIFT: Software Implemented Fault Tolerance", Ninth International Symposium on Fault Tolerant Computing, Madison, Wisconsin, June 1979.

(2) Daily, N., Hopkins, A. L., Jr., McKenna, J., Jr., "A Fault Tolerant Clocking System", Symposium on Fault Tolerant Computing, Palo Alto, CA, June 1973.

(3) Lanimer, S. J. and Maher, S. L., "A Continuously Reconfiguring Multi-microprocessor Flight Control System", AFWAL-TR-81-3070.

(4) Hecht, H., "Fault - Tolerant Software", IEEE Transactions on Reliability, Volume R-28, No. 3, August 1979.

(5) Melliar-Smith, M., Schwartz, R.L., "Hierarchical Specification of the SIFT Fault Tolerant Flight Control System", AGARD Symposium on Tactical Airborne Distributed Computing and Networks, June 1981.

(6) Sundstrom, D. E., et. al., "F-16 Multiplex: A Systems Perspective", Proceedings of the second AFCS Multiplex Data Bus Conference, Dayton, Ohio, October 1978.

(7) Hopkins, A. L., Brock, L. O., "Interim Report on Fault-Tolerant Aircraft Signal and Power Transmission Structures", C. S. Draper Laboratories, R-1298, Cambridge, Mass., August, 1979.

(8) "MIL-STD-1553 Multiplex Applications Handbook", Boeing Military Airplane Company, Contract F33615-78-C-0112, U.S. Air Force Systems Command (no publishing data given).

(9) Gross J., "Techniques for Interfacing Multiplex Systems", Air Force Wright Aeronautical Laboratories, Technical Report AFWAL-TR-80-1223, March, 1980.

(10) Military Standard, MIL-STD-1553A, "Aircraft Internal Time Division, Command/Response Multiplex Data Bus", 21 September 1978.

(11) AGARD Conference Proceedings No. 303, "Tactical Airborne Distributed Computing and Networks", AGARD-CP-303, June, 1981.

(12) McGough, J. G., Swern, F., "Measurement of Fault Latency in a Digital Avionic Mini-Processor", Bendix Corporation, Contract NAS1-15946, Report 3462, NASA Langley Research Center, October, 1981.

(13) Feller, W., "An Introduction to Probability Theory and Its Applications", Vol. I, Third Edition, Wiley & Sons, New York, 1968.

(14) Trivedi, K. S., Geist, R. M., "A Tutorial on the CARE III Approach to Reliability Modeling", Duke University, NASA Grant NAG1-70, NASA Langley Research Center, May, 1981.

(15) "Validation Methods Research for Fault Tolerant Avionics and Control Systems Sub-Working Group Meeting, CARE III Peer Review", NASA Conference Publication 2167, September, 1980.

(16) Stiffler, J. J., et. al., "CARE III Final Report", Vol. I (Report 159122), Vol. II (Report 159123), Raytheon Company, Contract NAS1-15072, NASA Langley Research Center, November, 1979.

(17) Heimbold, R. L., et. al., "Application of Advanced Electric/Electronic Technology to Conventional Aircraft", Lockheed-California Company, Contract NAS9-15863, Report N80-32375, NASA Johnson Space Center, July, 1980.

(18) Ness, W. G., McCrary, W. C., "Automated Reliability and Failure Effects Methods for Digital Flight Control and Avionic Systems" Vol. I, Vol. II, Lockheed-Georgia Company, Contract NAS2-10270, Report CR-166148, NASA Ames Research Center, March, 1981.

(19) Cunningham, T., et al, "Fault Tolerant Digital Flight Control with Analytic Redundancy", AFFDL-TR-77-25, May 1977.

(20) Boudreau, J. A., and Berman, H. L.; "Dispersed and Reconfigurable Digital Flight Control System", Volume 1, Tech Report AFFDL-TR-79-3125, December 1979.

(21) Grobert, K., et al, "Development of an Integrated Sensory System for Advanced Aircraft", To be published.

(22) Weinstein, W., "Development of an Advanced Skewed Sensory Electronic (ASSET) System For Flight Control", Grumman Aerospace Corporation, Report NADC 76295-30, October 1976.

(47) Leonard J.B.,Lecture No. 5, "Integration of Electrohydraulic Actuation Systems" one of six lectures at the AGARDshort course on Advanced Flight ControlActuation Systems, London, England and Dayton, Ohio, September 1981.

(48) Wyllie, C.E., "Overview of Honeywell Electromechanical Actuation Programs", presented at NASA Electric Flight Systems Workshop, Hampton, Virginia, June 1981

(49) Sperry Vickers In-House Study "Technological Trends of Flight Control Actuation Systems for Future Aircraft", April 1980.

(50) Cronin, Michael J., "The All Electric Airplane: Its Development and Logistic Support", NAECON. Dayton, Ohio, May 1981.

(51) Rowe, Stephen A., "Electromechanical Actuation Develoment Program (EADF)", NAECON, Dayton, Ohio, May 1981.

(52) Cronin, Michael J., "The All Electric Airplane as an Energy Efficient Transport", Paper No. 80111131, SAE Aerospace Congress and Exposition, Los Angeles, California, October 1980.

(53) Bird, Daniel K., "Three All Electric Aricraft", Paper No. ICAS-80-5.1, ICAS Meeting, Munich, Germany, October 1980.

(54) Leonard, John B., Sorensen, Theodore A., and Rowe, Stephen A., "Design Investigation of Electro-Mechanical Rotary Actuation Concepts for V/STOL Aircraft", NADC Technical Report No. NADC-78059-60, December 1979.

(55) Leonard, John B., Sorensen, Theodore A., and Rowe, Stephen A., "Analysis and Detail Design of Rotary Flight Control Actuator (ROTAC)", NADC Technical Report dNo. NADC-79093-60, March 1981.

(56) Clay, William C., "New All Electric System Technology", NAECON, Dayton, Ohio, May 1981.

(57) Wyllie, C.E., "Application of a Systems Approach to Design of Electro-mechanical Actuation Systems", NAECON, Dayton, Ohio, May 1981.

(58) Mehdi, Ishaque S., "Will Power-By-Wire Replace Power-By-Hydraulics?", NAECON, Dayton, Ohio, May 1981.

(59) Swingle, W.L. and Edge, J.T. "The Electric Orbiter", NAECON, Dayton, Ohio, May 1981.

(60) Bird, D.K., "Electromechanical Flight Control Actuation," SAE Paper No. 771004, Los Angeles, California, November 1977.

(61) Boldt, T. R., Shen, J.S., & Mehdi, I.S., "Airplace Actuation Trade Study, Phase I - Development of ATS Design Data Base, "Boeing Document D180-25487-1, March 1980.

(62) Boldt, T.R., et al "Airplane Actuation Trade Study, Phase II - Design of Two Airplanes", Boeing Document D180-487-2, September 1980.

(63) Rowe, S., "Electromechanical Airplane Actuation Trade Study," Airesearch Manufacturing Co., Document No. 80-17284, August 1980.

(64) Helsey, C.W., Jr., "Power-By-Wire For Aircraft - The all Electric Airplane," SAE Paper No. 771006, Los Angeles, California, November 1977.

(65) Chenoweth, C.C., et al "Integrated Actuation Package and its Application," Boeing Document D180-20225-1, August 1977.

(66) Demerdash, N.A. & Nehl, T.W., "Closed Loop Performance of a Brushless DC Motor Powered Electromechanical Actuator For Flight Control Applications," IEEE Transactions on Industry Applications, May/June 1980.

(67) Demerdash, N.A. & Nehl, T.W., "Numerical Simulation of Dynamics of Brushless DC Motors for Aerospace and Other Applications," Final Report on Virginia Polytechnic Institute and State University-NASA (JSC), Contract No. NAS9-15091, NASA-Johnson Space Center, Houston, Texas, 1978.

(68) Delco Electronics, "Final Report on the Electromechanical Flight Control Actuator," Contract No. NAS9-14952, General Motors Corporation, Delco Electronics Division, Santa Barbara Operations, Goleta, California, 1978.

(69) Bert Sawyer & J.T. Edge "Design of a Samarium Cobalt Brushless DC Motor for Electromechanical Actuator Applications," IEEE NAECON, Dayton, Ohio, May 1977.

(70) Phillips, J.W., "All Electric Sub-Systems for Next Generation Transport Aircraft," Lockheed-Georgia Company, AIAA Meeting, New York, August 1979.

(71) Swihard, John M., "The Next Generation Commercial Aircraft: The Technology Imperative," Boeing, ICAS Meeting, Munich, Germany, October 1980.

(72) Cronin, J.J., "Advanced Secondary Power System for Large Commercial Air Transport," LR28747, Lockheed-California Company, March 1979.

(73) Voight, Allan A., "Electric Flight Control System: Applicable Now!," General Dynamics Corporation, NAECON, Dayton, Ohio, May 1977.

(74) Heimbold, R.L., Lee, H.P. & Leffler, R.F., "Development of Advanced Avionics Systems Applicable to Terminal Configured Vehicle," NASA/ Lockheed NASI 15546, December 1979.

(75) Edge, J.T., "Electromechanical Actuator Technology Development Program," NASA-JSC, SAE Meeting, Cherry Hill, 1978.

(76) Wood, Neal E., "Advances in Primary Flight Control Actuation Using Electro-mechanical Actuator Technology," Airesearch, NAECON 1977.

(77) Lafuze, D.L., "Final Report on 150 KVA Sammarium Cobatl VSCF Starter/ Generator Electrical System," AFAPL/General Electric AFAPL-TR-78-104, December 1978.

(78) Demel, H.F., et al "Samarium Cobalt (SMCO), Generator/Engine Integration Study," AFAPL/General Electric Report No. AFWAL-TR-80-2022, April 1980.

(79) Wood, Echolds, & Ashmore "Electromechanical Actuation Feasibility Study," Air Force Flight Dynamics Laboratory, Report No. AFFDL-TR-76-42.

(80) Grau "Feasibility Investigation for Advanced Flight Control Actuation Systems; All Electric Concepts (AFCAS/AE)," Naval Air Development Center, Technical Report No. NADC 76160-30.

(81) Edge, "An Electromechanical Actuator Technology Development Program," SAE Technical Paper 780581.

(82) Rowe, "Electromechanical Airplance Actuation Trade Study", Airesearch Manufacturing Company of California, Report No. 80-17284.

(83) Wood & Lewis, "Electromechanical Actuation Development", Air Force Flight Dynamics Laboratory, Report No. AFFDL-TR-78-150.

(84) Lewis, Gray & Wood, "Electromechanical Actuation Development", Air Force Flight Dynamics Laboratory, Report No. AFFDL-TR-80-3024.

(85) Jones, D. R., "Study of Technological Trends of Flight Control Actuation Systems for Future Aircraft," Sperry Vickers In-House Study/Report, April, 1980.

(86) Leonard, J.B., "Actuation Systems Study - Addendum to ISS Study," Grumman Aerospace Corp. Report No. G-GCR-78-002, July, 1978.

(87) Koch, W.C., Research and Development of an Integrated Servo Actuator Package for Fighter Aircraft," AFFDL Report No. AFFDL-TR-69-109, November 1969.

(88) Marx, M.F., and Lewis, T.D., "Electromagnetic Force Motor Desing Using Rare Earth-Cobalt Permanent Magnets. Paper Presented at IEEE 1977 National Aerospace and Electronics Conference (NAECON) Dayton, Ohio, May 1977.

(89) Jenney, G.D., "Research and Development of Aircraft Control Actuation Systems - The Development of a Direct Drive Fly-By-Wire Flight Control System and Evaluation of a Force Sharing Fly-By-Wire Actuation," AFFDL-TR-77-91, September 1977.

(90) "Feasibility Study for Advanced Flight Control Actuation System (AFCAS)," Report NR72H-240, Columbus Aircraft Division of North American Rockwell, June 1972.

(91) Demarchi J.N. and Haning, R.K., "Control-By-Wire Modular Actuator Tests (AFCAS)," Report No. NADC 75H-1, Columbus Aircraft Division of Rockwell International, January 1975.

(92) Demarchi, J.N. and Haning, R.K., "Design and Fabrication of an 8000 P.S.I. Control-By-Wire Actuator for Flight Testing in a T-2C Airplane," Columbus Aircraft Division of Rockwell International, January 1976.

(93) Becker, K.F. and Pederson, N.F. "Design and Development of a Lateral Axis Integrated Actuator Package for Tactical Fighter Aircraft," Vickers A-O-M Division of Sperry Rand Corporation, AFFDL-TR-73-26, February 1973.

(94) Shen, T.S., "The Integrated Actuator Package (IAP) and Its Applications to the Flight Control System of Military and Civil Transport Aircraft", June 1977, Boeing Report #D180-20225-1.

(95) Earley, B.H., "Objectives for the Design of Improved Actuation Systems", AGARD-AG-224, April 1977.

(96) Jenney, G.D., "Research and Development of Aircraft Control Actuation Systems", AFFDL-TR-77-91, September 1977.

(97) Hogan, D., and Rinde, J.E., "Development of Direct Drive Control Valve for Fly-By-Wire Flight Control System Actuators", AFFDL-TR-78-32, March 1978.

(98) Graw, R., "Feasibility Investigation for Advanced Flight Control Actuation Systems; All Electric Concepts (AFCAS Z-Z)", NADC-76160-30, March 1976.

(99) Demarchi, J.N., and Haning, R.K., "Flight Verification of the Advanced Flight Control Actuation System (AFCAS) in the T-2C Aircraft", NAVAIRDEVCEN 75287-60, June 1978.

(100) Air Force Flight Dynamics Laboratory, "General Design Criteria for Hydraulic Power Operated Aircraft Flight Control Actuators", AFFDL/FGL-TM-78-73, June 1978.

APPENDIX A

BUS LOADING ESTIMATES

Bus loading estimates were obtained from data acquired from three sources:

1) F-16 Avionics

   Sundstrom, D.E., et al, "F-16 Multiplex: A Systems Perspective", Proceedings of the 2nd AFCS Multiplex Data Bus Conference, Dayton, Ohio, October, 1978.

2) Avionics and Flight Control

   Hopkins, A.L., Brock, L.O., "Interim Report on Fault-Tolerant Aircraft Signal and Power Transmission Structures", C.S. Draper Laboratories, Cambridge, Mass., R-1298, August, 1979.

3) Flight Control System, DC-10 Stretch Airplane

   Bendix Proposal to Douglas Aircraft Company for DC-10 Stretch Airplane, 1979.

Groundrules For Bus Loading Calculations

In deriving bus loading estimates we will be conservative and assume, in all cases, RT to RT communications. In particular, the broadcast mode will not be used for purposes of bus loading estimates. A 1 MHz bit rate is assumed, throughout.

In a typical RT to RT request/reply transfer define

RT_A = transmitting RT

RT_B = receiving RT

BC = bus controller.

Then the request/replay sequence and timing is

1) BC issues "Receive Cmd" to RT_B = 20 μsec
2) BC issues "Transmit Cmd" to RT_A = 20 μsec
3) Response time = 12 μsec
4) RT_A issues "Status" = 20 μsec
5) RT_A issues "Data" = 20 μsec
6) Response Time = 12 μsec
7) RT_B issues "Status" = 20 μsec
8) Gap between messages = 2 μsec

Let N = Number of data words per second transmitted

M_K = Number of messages per second of K words each.

Then

$$N = \sum_{K=1}^{N} K M_K$$

and $\sum_{K=1}^{N} M_K$ = Number of messages per second transmitted.

The proportion of bus usage is the

1) $r = (106 \times \sum M_K + 20N) \times 10^{-6}$

or

2) $r = N \left(\frac{106}{W} + 20\right) \times 10^{-6}$

where

$$W = \frac{N}{\sum M_K} = \text{average number of words per message.}$$

F-16 Avionics

For this system (From Table III of Reference 1)

$N = 14{,}405$ words/sec, excluding polling

$\sum M_K = 1339.0625$ messages/sec.

This system comprised several types of data transmission, e.g.,

BC to RT, RT to BC and RT to RT.

In the bus loading estimates we assumed that all transmissions were RT to RT since this resulted in the most conservative estimates.

From N and $\sum M_K$ we compute

$$W = \frac{N}{\sum M_K} = 10.76 \text{ words/message}$$

and, from (2),

$$r = 14{,}405 \left(\frac{106}{10.76} + 20\right) \times 10^{-6} = 0.43.$$

Then, avionics bus utilization is 43%.

Avionics and Flight Control (Hopkins and Brock)

From Table 4-9 in the referenced document we obtain

$N = 9662$ words/sec.

This data includes both the flight control and avionics systems and the levels of redundancy judged to be required by the authors. If we assume

- a redundant signal is only transmitted to a single RT (i.e., and not to multiple users) and
- W = 12 words/message, on the average

then

$$r = 9662 \left(\frac{106}{12} + 20\right) \times 10^{-6} = 0.279.$$

Then, bus utilization is 27.9%.

This estimate appears to be excessively optimistic. The authors postulate sampling rates of the order of 50/second for flight controls. Since flight control algorithms (e.g., inner loop) are generally iterated at 50/sec the authors evidently assumed that data would be made available on request, thus eliminating any transport delay between inputting and using the data. If data transmission is not synchronized to user request then the rate of transmission should be at least 4 times greater than the iteration rate.

Anoter factor that must be considered is the number of subsystems using a redundant variable. Our estimates assumed that a simple variable was transmitted to a single subsystem and that this counted for one transmission. This is justified only if the broadcast mode is acceptable. If not, then a redundant variable might have to be transmitted separately to each user of the data.

DC-10 Stretch Flight Controls

The flight control system included autopilot/flight director, Cat IIIa autoland, autothrottle and stability augmentation. The system contained two, dual-dual computer systems, one for flight guidance and the other for flight augmentation. The data transmission requirements were:

SUBSYSTEM	WORDS/FRAME	ITERATION RATE	WORD/SEC
FGC #1 (DUAL)	124	10/sec	1240
FGC #2 (DUAL)	124	10/sec	1240
FAC #1 (DUAL)	124	20/sec	2480
FAC #2 (DUAL)	124	20/sec	2480
			7440 TOTAL

Assuming that it is necessary to transmit variables at a rate at least 4 times greater than the iteration rate then the total words/sec required is

29,760 words/sec.

If we assume an average of 12 words/message than

$$r = 29{,}760 \left(\frac{106}{12} + 20\right) \times 10^{-6} = 0.86.$$

Thus, bus utilization is 86%.

This estimate is realistic and conservative, e.g., it assumes

- a single 1553B bus
- 2 quadruplex I/O's
- no broadcast transmissions
- a transmission rate equal to 4 times the iteration rate.

APPENDIX B

MAINTENANCE REQUIREMENTS FOR APPLICATIONS PROCESSORS

Because of the simplicity of the communication network and the ease of incorporating spares, the primary measure of maintainability is the number of spares that must be carried in order to obtain a desired maintenance period.

The number of spares required will depend upon the maintenance strategy employed, i.e.,

- scheduled or unscheduled maintenance,
- powered or unpowered spares.

Thus, we consider four maintenance strategies:

Strategy #1: scheduled, powered spares

Strategy #2: scheduled, unpowered spares

Strategy #3: unscheduled, powered spares

Strategy #4: unscheduled, unpowered spares.

In scheduled maintenance, maintenance is performed at prescribed intervals of time. The system must maintain its integrity between maintenance periods. In unscheduled maintenance, maintenance is performed whenever system integrity is likely to be compromised by subsequent failures.

Ground Rules

Maintenance requirements are estimated for a single, redundant subsystem.

- Biannual maintenance period = 1500 hours.
- r = minimum number of redundant elements required to achieve 10^{-10}/hour.

- m = number of spares
- 3-fold voting. When a fault is detected the affected element is immediately isolated and disengaged without any degradation in performance. Thus, loss of subsystem function occurs when and only when all elements but one have failed. This assumption applies to most subsystems but not to all e.g., skewed sensors.

To simplify the calculatins it is assumed that spares, powered or unpowered, are brought on-line at the instant an active element fails. In practice, unpowered spares would be brought on-line after each flight, as required.

To further simplify the calculations it is assumed that the minimum number of elements required for 10^{-10}/hour is four, i.e., r = 4. This is based on the observation that the failure rate of a typical avionics processor is of the order of 300 x 10^{-6}/hour (MTBF = 3333 hours) and thus it requires four such processors to obtain 10^{-10}/hour survivability.

Maintenance requirements will be determined for a range of subsystems having individual element failure rates of

$\lambda_1 = 300 \times 10^{-6}$/hour

$\lambda_2 = 100 \times 10^{-6}$/hour

$\lambda_3 = 50 \times 10^{-6}$/hour

Mathematical Preliminaries

The maintenance estimates were obtained from a simple Markov chain representation of the failure events. The chain is shown in Figure 56 where

E_0 = event of no failed elements

E_k = event of K failed elements, K = 1, 2, ..., ℓ - 1

E_ℓ = event of $\underline{\ell}$ or more failed elements

$P_k(n)$ = occupancy probability for state E_k at time n.

q_k = transition probability from state E_{k-1} to E_k

Each transition corresponds to a flight of one hour.

The chain is only an approximation to the actual failure process since it does not account for multiple failures in a single flight. However, a comparison between the correct result for strategy #1 and results obtained using the Markov chain indicates that the errors are negligible for the range of parameters involved.

From Figure 56 we derive the following difference equations:

$$P_0(n) = (1 - q_1)\, P_0(n - 1)$$

$$P_1(n) = (1 - q_2)\, P_1(n - 1) + q_1\, P_0(n - 1)$$

.
.
.

B1)

$$P_{\ell-1}(n) = (1 - q_\ell)\, P_{\ell-1}(n - 1)\, q_{\ell-1}\, P_{\ell-2}(n - 1)$$

$$P_\ell(n) = P_\ell(n - 1) + q_\ell\, P_{\ell-1}(n - 1)$$

subject to the initial conditions

$$P_0(o) = 1$$

$$P_k(o) = 0,\ K = 1, 2, \ldots, \ell.$$

It is easy to show that the mean time from entry into state E_{k-1} to entry into state E_k is $1/q_k$. Thus, the mean time to entry into state E_ℓ is

B2) $$N_{avg} = \frac{1}{q_1} + \frac{1}{q_2} + \ldots + \frac{1}{q_\ell} \quad .$$

In the case when $q_k = q$, $K = 1, 2, \ldots, \ell$,

B3) $$N_{avg} = \frac{\ell}{q}$$

Strategy #1

The probability of loss of subsystem after n flights is $P_{m+r-1}(n)$ where we have set $\ell = m + r - 1$. The average probability of loss of subsystem per hour is

$P_{m+4-1}(n)/n$. For this strategy

$q_1 = (m + r)\lambda$

$q_2 = (m + r - 1)\lambda$

.
.
.

$q_{m+r-1} = 2\lambda$.

$\frac{P_{m+r-1}(n)}{n} = 10^{-10}$ was solved for n and m

and the results plotted in Figure 57 for λ_1, λ_2 and λ_3.

Strategy #2

Same as Strategy #1 except that

$q_1 = q_2 = \ldots = q_m = r\lambda$ $(r = 4)$

$q_{m+1} = r\lambda$

$q_{m+2} = (r - 1)\lambda$

.
.
.

$q_{m+r-1} = 2\lambda$.

The results are plotted in Figure 57.

Strategy #3

In Strategies #3 and #4 a maintenance action will be performed, as performed, as required, i.e., after the loss of m spares. As a measure of maintenance action we want to compute the

- n_{avg} = mean time to loss of m spares and
- p_m (1500) = probability of loss of m or more elements in 1500 hours or, equivalently, the probability of at least one maintenance action in 1500 hours.

Thus, the intention is to obtain a value of $n_{avg} \geqq 1500$ while at the same time insuring relatively infrequent maintenance action in that time period.

In Strategy #3

$q_1 = (m + r)\lambda$

$q_2 = (m + r - 1)\lambda$.

.
.
.

$q_m = (r + 1)\lambda$

Figure 58 shows Pm (1500) versus m for λ_1, λ_2, and λ_3.

Figure 59 shows n_{avg} versus m for λ_1.

Strategy #4

Same as Strategy #3 except that

$q_1 = q_2 = \ldots = q_m = r\lambda$ $(r = 4)$

and

$$n_{avg} = \frac{m}{r\lambda} .$$

Figure 60 shows P_m (1500) versus m for λ_1, λ_2, and λ_3.

Figure 61 shows n_{avg} versus m for λ_1. The mean for λ_2 and λ_3 can be obtained by multiplying n_{avg} by the factors 3 and 6, respectively.

Distributed Versus Central Processing

It is interesting to compare the relative survivability of distributed versus centralized processing. Assume that we are given m, distinct, flight critical tasks. Assume further that each task must be 4-fold redundant for 10^{-10}/hour survivability. In a distributed system each task is assigned to a dedicated microprocessor for a total of 4 m such processors. In a centralized system, on the other hand, the m tasks would

be assigned to a single processor. Naturally such a processor would require more computing power and memory and would, as a consequence, have a larger failure rate than a microprocessor. If

λ_d = failure rate of a single microprocessor

λ_c = failure rate of a single, centralized processor

then the probability of loss of system in one hour is

B4) $S_d = m\,(4\lambda^3_d + \lambda_d^4)$

for the distributed system and

B5) $S_c = 4\lambda^3_c + \lambda_c^4$

for the centralized system.

If $\lambda d << \lambda c$ then the survivability of the distributed system can be considerably less than that of the centralized system. As an example, let

$m = 5$ tasks

$\lambda_d = 50 \times 10^{-6}$/hour

$\lambda_c = 300 \times 10^{-6}$/hour.

Then

$S_d = 2.5 \times 10^{-12}$/hour

and

$S_c = 1.08 \times 10^{-12}$/hour.

Of course 20 microprocessors are required as compared with only 4, centralized processors. Further, the ratio of the respective failure rates ($\lambda d/\lambda c$) is critical in determining the relative survivability.

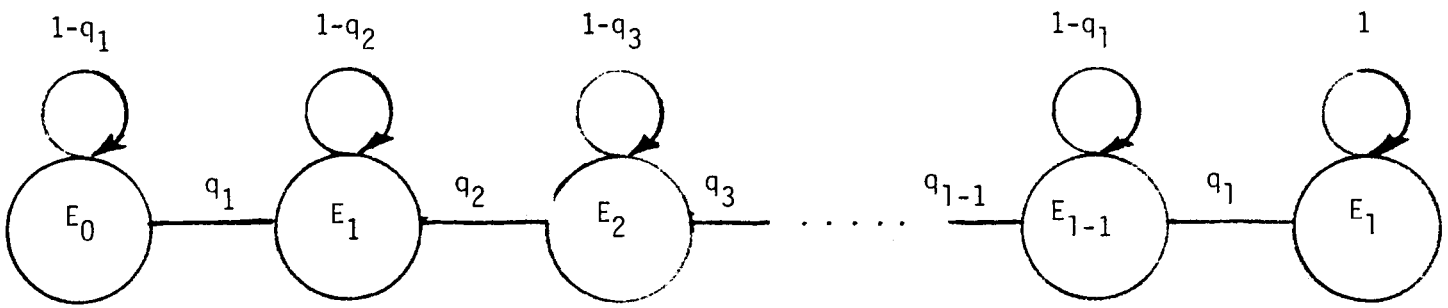


Figure 56 **Markov Chain Representation for Failure Events**

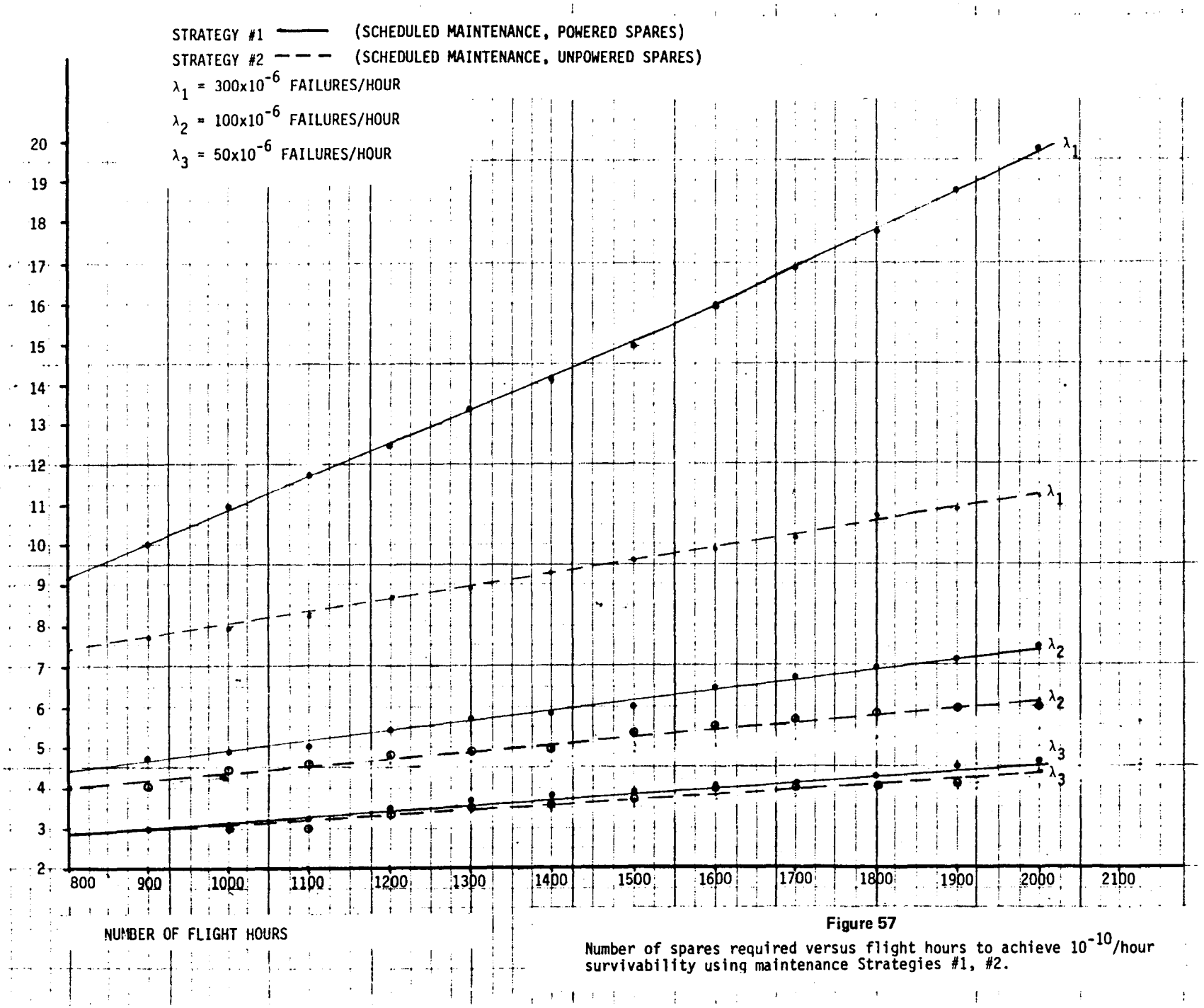


Figure 57

Number of spares required versus flight hours to achieve 10^{-10}/hour survivability using maintenance Strategies #1, #2.

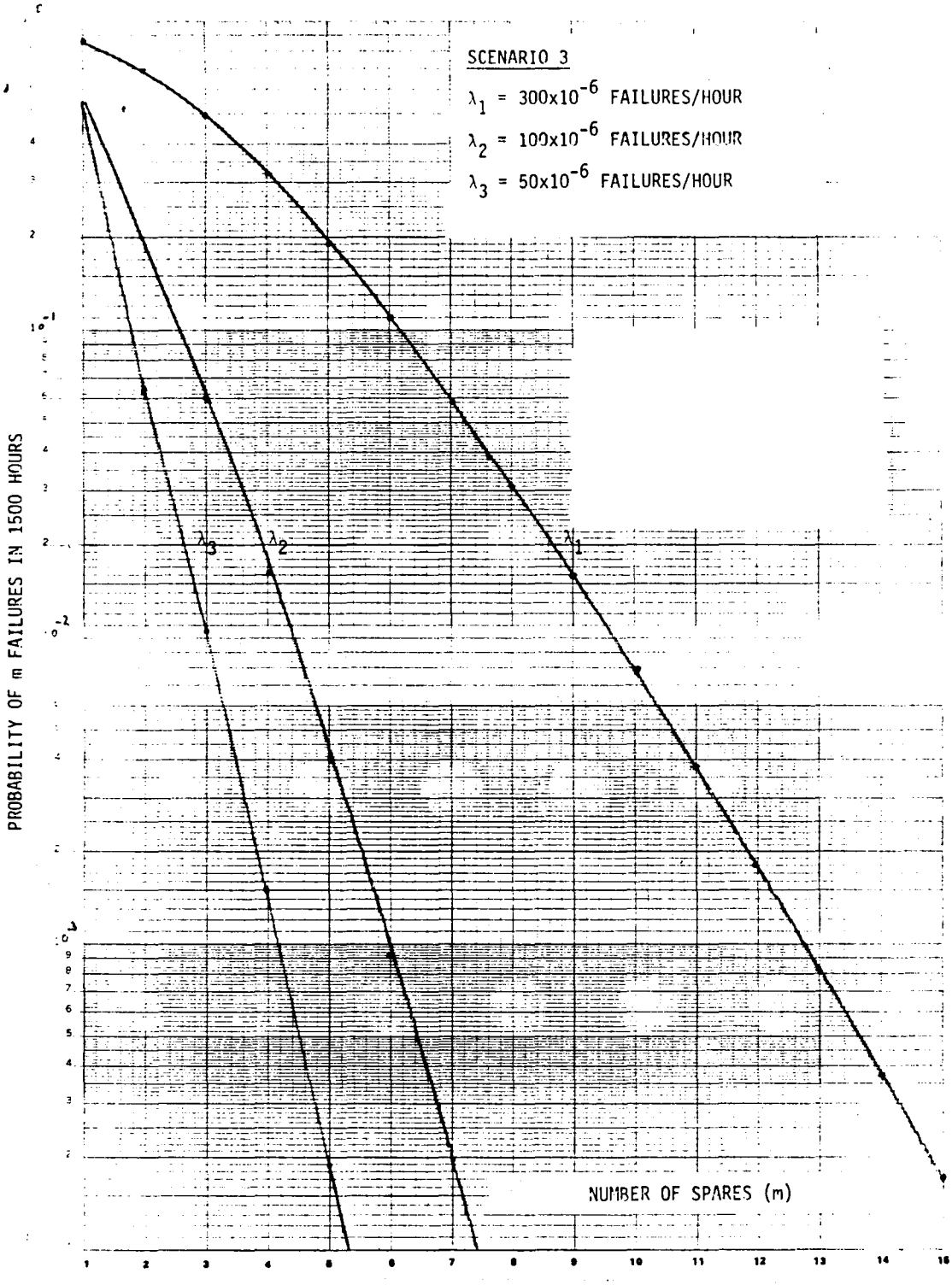


Figure 58 **Probability of m Failures in 1500 Hours Versus m**
(for Strategy #3, Unschedules, Powered Spares)

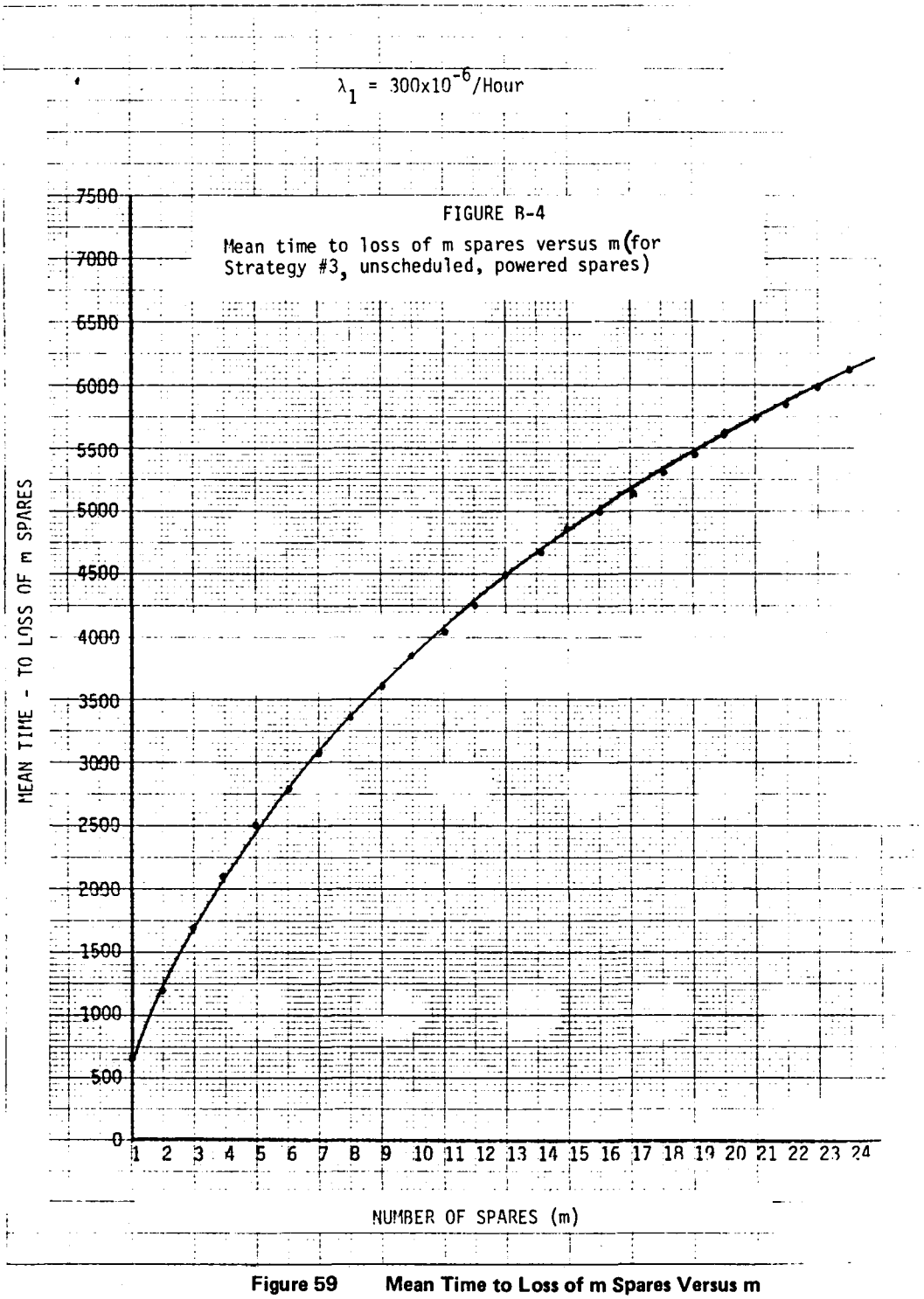


Figure 59 Mean Time to Loss of m Spares Versus m (for Strategy #3, Unscheduled, Powered Spares)

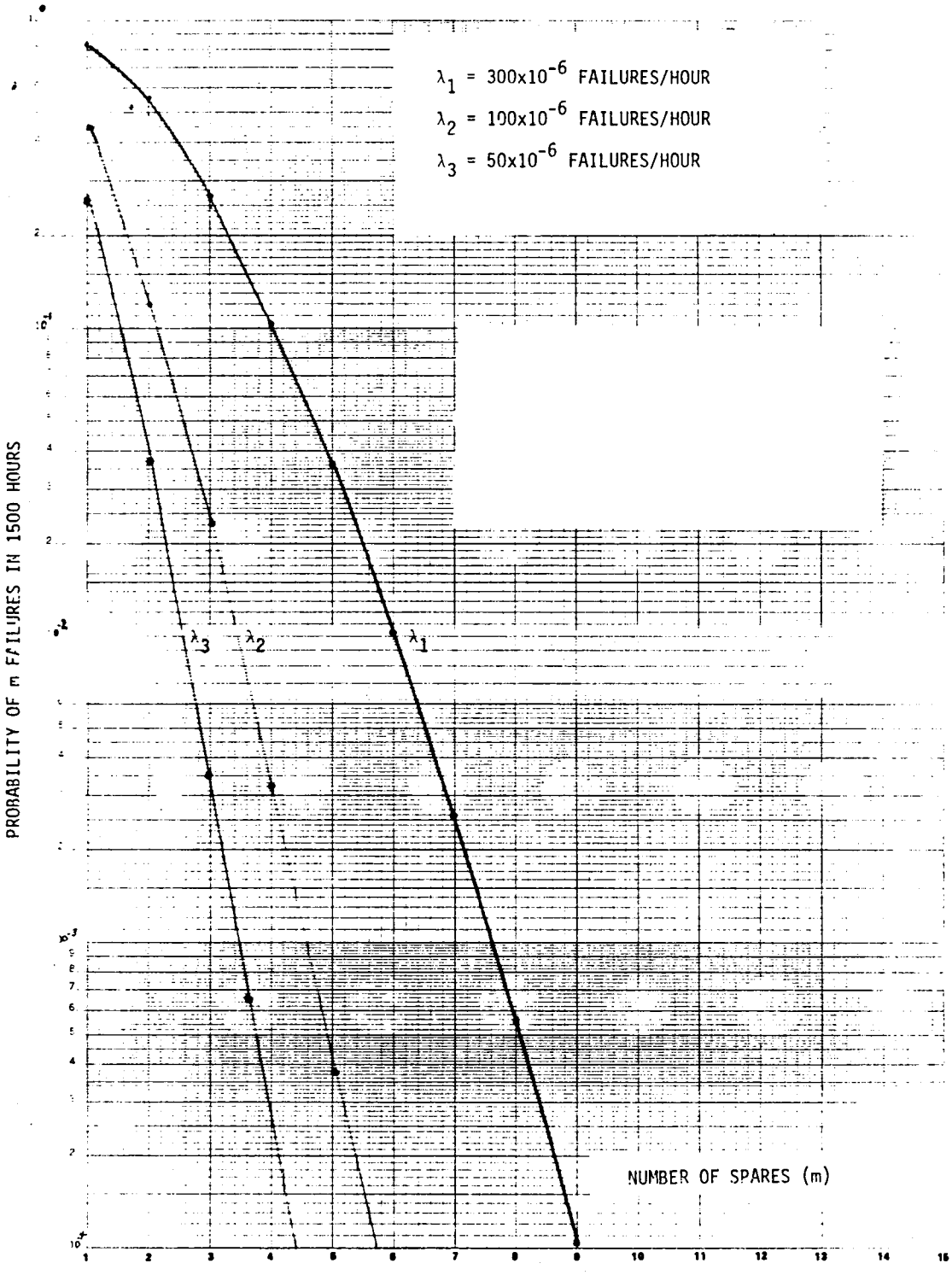


Figure 60 Probability of m Failures in 1500 Hours Versus m (for Strategy #4, Unscheduled, Unpower Spares)

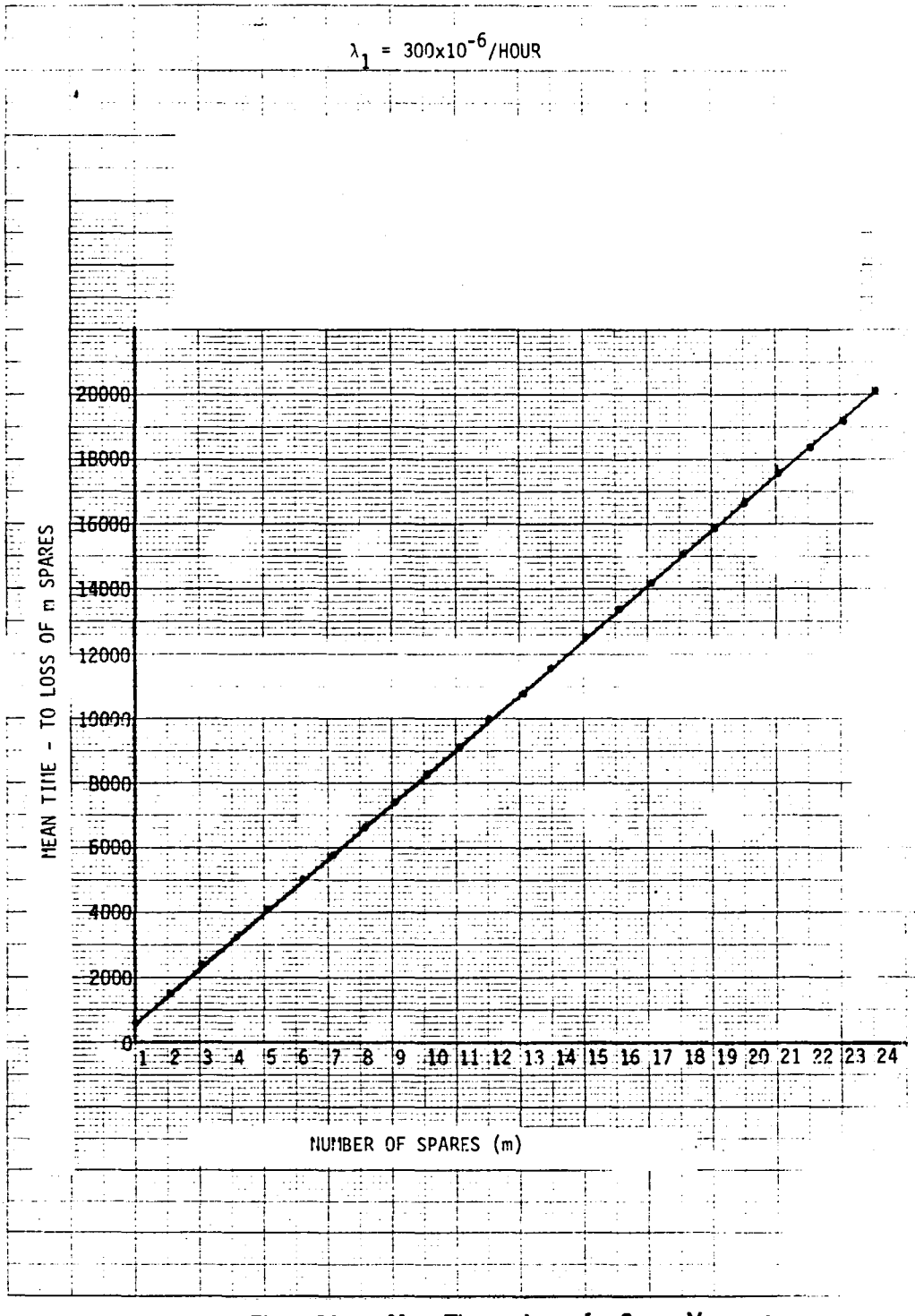


Figure 61 **Mean Time to Loss of m Spares Versus m**

(for Strategy #4, Unscheduled, Unpowered Spares)

APPENDIX C

CLOSED-LOOP TEST FACILITY

1. INTRODUCTION

Bendix has developed a closed-loop test facility to provide an experimental medium which can be used through every phase of the program either as a design tool or to validate the design.

Experience has shown that errors are relatively easy to detect and correct if they are identified early in the program and before the affected modules are integrated into larger modules.

2. APPLICATION OF THE CLOSED-LOOP FACILITY

The closed-loop facility can be used in a variety of ways:

- Preliminary Design tool

  The facility can be used to assist the designer in the initial selection of filter algorithms, word size, iteration rates; or in the assessment of synchronous versus asynchronous operation, quantization effect, intersample ripple, etc.

- Validation and Performance

  Once the preliminary design is established the facility can be used to validate performance such as:

  - intersample response
  - quantization effects
  - finite word size effects
  - overflow
  - monitoring thresholds
  - open-loop/closed-loop phase, amplitude, frequency
  - effects of computational delays
  - effects of asynchronous computation (if applicable)
  - time responses
  - equalization, signal selection, failure detection

- Integration Testing

  Because the facility can accommodate multiple computers, it is an ideal facility for integration testing.

- Provides Normal Access to Computers

  In addition to providing a software development system the facility features a monitor program which allows an operator sitting at a CRT console to exercise control over the simulator. The facility also provides direct access to one or more processors either singly or simultaneously. For example, 1) the content of designated memory locations in one or more processors can be displayed continuously on the console or 2) designated memory locations in one or more programs can be changed either singly or simultaneously via the console. For maximum flexibility the monitor permits the user to construct virtually any display format desired.

3. COMPONENTS OF THE CLOSED-LOOP TEST FACILITY

Figure 62 shows the major hardware components. Although the figure shows a dual Flight Control Computer (FLCC), the present facility can accommodate up to eight computers. Specifically, the hardware and software components consist of:

Hardware Components

1) Data General Eclipse S/230 System

   - Eclipse S/230 CPU
   - 32K or 64K words of memory
   - 10 megabyte disc assembly
   - diskette drive
   - video display console
   - line printer

   This unit contains software for plant modelling, BDX-930 communications and operator control.

2) BDX-930/Eclipse Software Development System Interface

   This unit provides the hardware necessary to access up to 8 flight control BDX-930 computers. It provides the conventional features of an access panel and in addition provides:

- single or simulataneous memory access, either storing or fetching, of up to 8 Flight Control Computers
- single or simultaneous control of up to 8 Flight Control Computers

3) I/O Simulator

This unit provides the hardware necessry for communication between the Flight Control Computers and the Eclipse S/230. For example, it converts DC analog outputs from the Flight Control Computers to appropriate digital formats which are then transmitted, on command, to the Eclipse. Specifically, the unit contains (See Figure 63):

BDX-930 with 16K of Memory
2 - 1553B Bus Controllers and Bus Interfaces
AD and DA Converters
I/O Controller
DC Inputs
AC Inputs
DC Outputs
AC Outputs
Synchro Inputs
Synchro Outputs
Discrete Inputs
Discrete Outputs
Intercomputer Serial Data Links

The BDX-930 can be used in a variety of ways to enhance the simulation capabilities, e.g.

Formatting input and output variables
Emulating fault conditions on sensors, actuator commands, etc.

In addition, it can be used to emulate a single Flight Control System in lieu of the target system. This allows for an early evaluation of control modes and single system operation.

4) Jack Panel, Power Supplies

Software Components

1) Plant Model (Resident in Eclipse)

- 6 DOF Linear, Perturbation Airframe
- Sensor/Actuator Dynamics

- Bending Modes
- Prefilters, if Slow Clock Rate is used
- 12 MS/Iteration

2) Monitor Program (Resident in Eclipse)

- Interactive with Operator
- Functions as Access Panel to Flight Control Computers
- Memory Loads 8 BDX-930's Simultaneously
- 50 MS/Word of Transfer, MAX
- Accesses all System Variables in FLCC's or I/O Simulator
- Displays Selectable Data Sets
- Provides Complete Control over Simulation

3) I/O Simulator (Resident in BDX-930 of I/O Simulator)

- Services FLCC's I/O
- Simulates Redundant Sensors/Actuators
- Simulates Sensor Faults
- Outputs to Recorder, Eclipse, CRT Console
- Control Laws if Target FLCC Unavailable

4) OFP Software (Resident in FLCC)

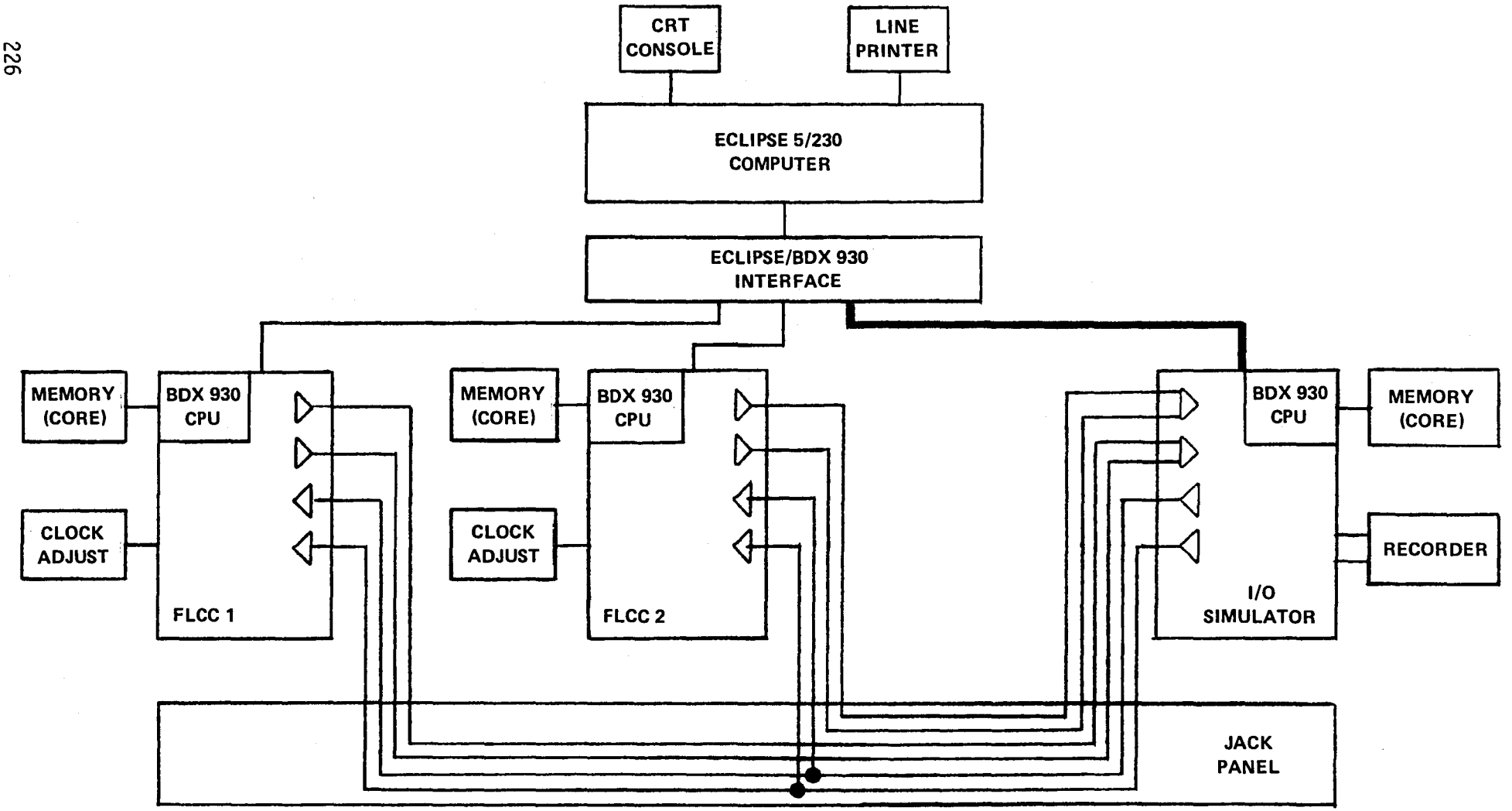


Figure 62 Closed Loop Test Facility

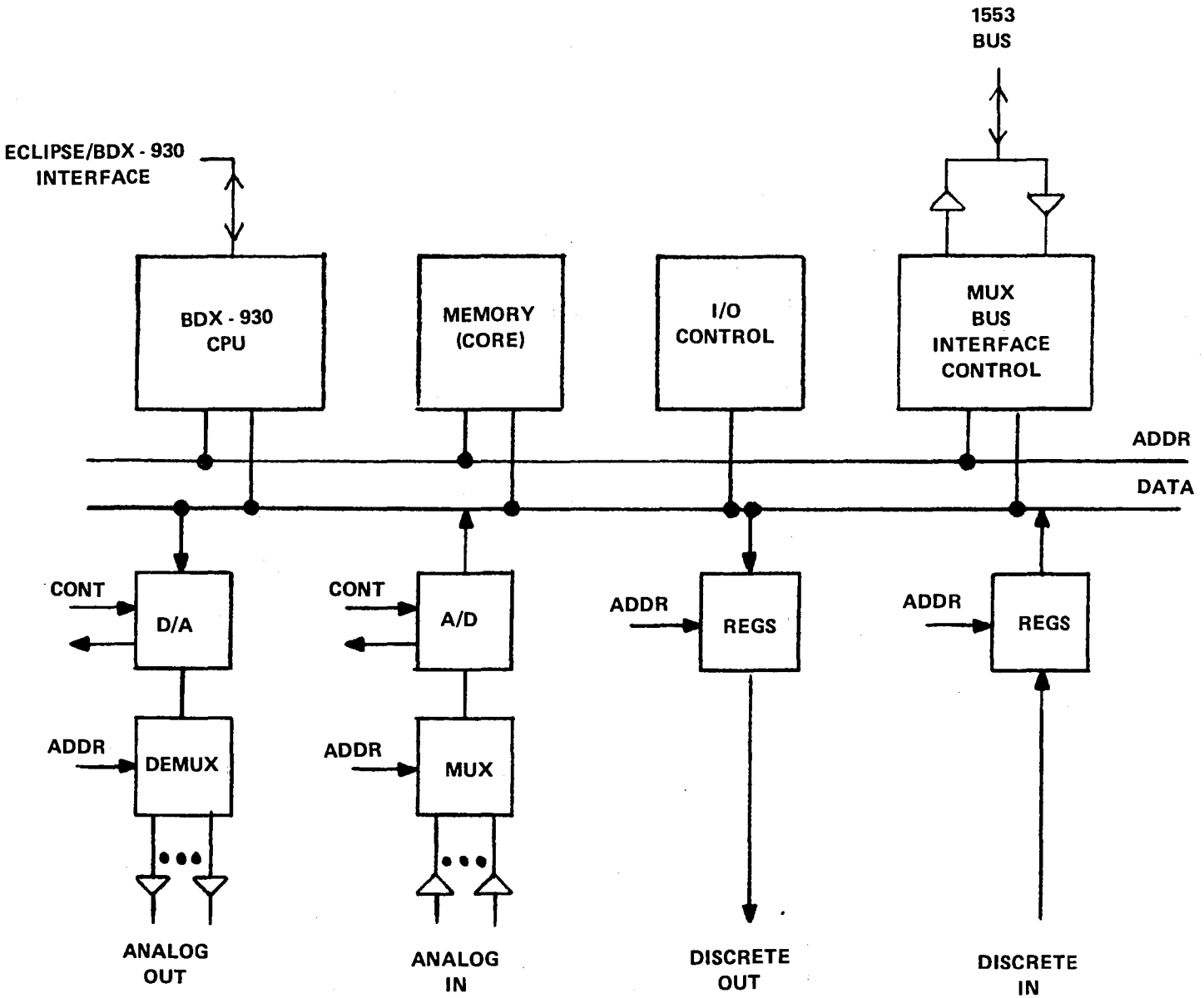


Figure 63 I/O Simulator

APPENDIX D

INTEGRATED SENSOR TECHNOLOGY

The design of advanced flight control systems (FCS), particularly digital fly-by-wire FCS, requires highly reliable communication paths to meet the overall FCS reliability. In addition to redundant onboard computers and output devices, redundant sensory data are required. The use of conventional approaches to satisfy the sensory requirements leads to a proliferation of hardware with the attendant reliability, weight, power, maintenance, and cost penalties.

An Integrated Sensory Subsystem (ISS) for advanced high-performance aircraft, consists of redundant inertial sensors, air data probes, and other transducer/sensory data in combination with a digitally implemented Redundancy Data Management System (RDMS) and computational algorithms to provide accurate, reliable vehicle sensory data to several using subsystems. For example, the information generated by the ISS (which includes rate, acceleration, attitude, heading, and air data parameters), is utilized by the control laws of the DFCS and by other aircraft subsystems such as the Engine Controls, Displays, and Navigation systems.

The major objective of the ISS is a sensory subsystem that:

- Satisfies the mission and flight safety reliability and redundancy requirements of fly-by-wire FCS by using redundant sensors and reconfigurable functional data paths embedded within the Data Handling System (DHS).
- Decreases vulnerability to interior damage by dispersal of components.
- Minimizes logistic support (1) by the use of equipment configured from more finely partioned interchangeable modules, with a common electrical interface; (2) by the elimination of dedicated equipment such as Attitude and Heading Reference systems and Air Data Computers; and (3) by the use of skewed inertial sensor technology to minimize hardware proliferation.
- Eliminates intermediate-level maintenance through the use of a failure detection and isolation system within the ISS that fault-isolates down to the module level.

The conceptual design of the ISS includes skewed/dispersed inertial sensors, dispersed air data probes and transducers, and the DHS which includes the algorithms to perform fault isolation, dispersed sensor compensation, and best-estimate output data computations.

ISS DESIGN

The ISS uses design techniques that:

- Maximize the use of mature sensor technology, modularization and interchangeability.
- Maximize the capability of self-contained fault detection and isolation.
- Provide sensor configurations that reduce the time needed for scheduled and unscheduled maintenance.
- Utilize dispersed sensor configurations that insure a survivable sensor system.

The ISS system is composed of three main elements:

- A sensor set consisting of hard mounted, skewed, and dispersed rate integrating gyros and accelerometers; low and high speed air data probes which are located in close proximity to modularized air data transducers: an Inertial Navigation System (INS), pilot command sensors, surface position sensors, radio navigation devices, terminal guidance sensors and landing aids. The ISS concept is shown in Figure 64.
- A reliable and survivable input-output (I/O) bus that links the sensory data to three or more flight control computers.
- A computation network within the flight Control System complex consisting of subroutines that provide:
  - Sensor signal selection through failure detection and isolation algorithms.
  - State estimation and sensor data normalization algorithms to account for the effects of deterministic errors associated with the dispersed sensors and random sensor noise.

- Strapdown attitude and heading computations.

- Air data computations for Mach number, true airspeed, etc.

The ISS sensor set consists of:

- Redundant skewed arrays of strapdown integrating rate gyros and accelerometers.

- Redundant air data probes and transducers.

- Magnetic heading reference sensors.

- Nav/guidance equipment including an inertial navigation system and radio aids.

- Command inputs/surface position transducers.

Six gyros and six accelerometers are configured in conical arrays to provide a two-fail operational sensor configuration. The instruments are dispersed to assure a survivable system. The cone axis for the gyros lies along the aircraft longitudinal axis and the accelerometer cone axis lies along the aircraft yaw axis. The orientation of the cone axes and selection of cone angles is based upon the maximum rate or acceleration that is anticipated in each axis, and the axis about which the maximum level typically occurs. Details of this selection process are given in (ref. 23, 24) and Appendix E.

The ISS design philosophy for inertial sensor packaging and dispersion for survivability permits installation of gyros and accelerometers in less than ideal locations with respect to bending nodes/antinodes and the aircraft C.G. The appropriate compensation generated by the use of a state estimator can eliminate flight control system/bending mode coupling and/or nuisance trips of the RDM failure detection routines. The configuration of the gyro and accelerometer RDM routines and the state estimator is shown in Figure 65.

In addition to providing feedback signals for flight control system stabilization, the inertial instruments provide the reference data for computing attitude and heading, thus eliminating the need for a dedicated AHRS. To minimize the overall hardware complement, inertial sensors and associated electronics are packaged in Inertial Component Assemblies which are dispersed onboard the aircraft as shown in Figure 66.

The air data portion of the ISS consists of a triple channel of air data probes and pressure transducers plus a fourth channel of air data parametres which are derived analytically.

The air data hardware configuration for conventional flight is shown in Figure 67. The probes and pressure transducer sets are remotely located from one another to assure system integrity with exterior damage. The pneumatic air data probes are of the multipurpose variety which sense static pressure, total pressure, and differential pressure for angle-of-attack (α) computations. The nose probe also provides differential pressure for sideslip (β) computations. The air data probes are linked to pressure transducers via short pneumatic tubing runs to minimize (1) the transport lag and (2) vulnerability to damage.

An independent probe and two dual total temperature probes complete the set of required air data probes. It should be noted that an additional source is available from the difference between left and right static pressure.

State-of-the-art pressure transducers are mounted in a Universal Transducer Assembly which, in addition to pressure transducers, contains a microprocessor for data preprocessing and data output control, a power supply, and I/O electronics.

In order to provide accurate long-term heading, flux valves are utilized. The flux valve data and gyro-derived heading data are combined via a complementary filter in the DHS to eliminate gyro-induced heading errors.

The navigation equipment and guidance data within the ISS consists of an inertial navigation system and the radio aids necessary to solve landing/guidance solutions.

The final set of ISS sensory data consists of the various FCS command and surface position transducers, including feedback signals to perform inidividual channel failure monitoring.

DATA HANDLING SYSTEM

The DHD depicted in Figure 68, is contained in the redundant computer complex and contains algorithms to perform the following functions:

- Normalization of the sensed parameters.
- Redundancy data management.
- ISS output parameter computation.

Normalization compensates the individual sensed parameters for local aircraft installation characteristics. The normalized data are theoretically equal and represent actual aircraft parameters. For example, air data parameters at each probe location are compensated for local pressure disturbances/variations which are functions of Mach, α and β. Gyro and accelerometer data are also normalized by use of a state estimator which provides compensation for local body bening and lever arm effects.

The sensor RDM, depicted in Figure 69, performs failure monitoring, failure isolation, and signal selection. In addition, analytic redundancy calculations are performed to minimize overall hardware requirements. for example, to achieve a two-fail operational set of air data parameters, a fourth channel of pressure ratio, α and β are derived from a set of filters using inertial navigation data and valid air data parameters.

The failure monitoring performed consists of two types: (1) a reasonableness test and (2) comparison between channels. The reasonableness test compares the latest calculated parameter with the previously calculated parameter. The failure threshold is a function of aircraft dynamics and short-term noise characteristics of the calculated parameter. Thus, the threshold associated with static pressure data is a function of the aircraft's maximum change in altitude, plus the short-term noise characteristics of static pressure data that occur between successive computation cycles. If the parameter exceeds the failure threshold a transient failure is declared, and the associated data is not utilized in subsequent calculations until the rate of change of the parameter falls below the failure monitor threshold.

Failure monitoring performs comparisons between channels based on the most current data. Should a parameter exceed the failure threshold for a specific length of time, a permanent failure is declared.

The Redundancy Management program for six skewed sensors contains: a Transient Failure Removal Routine, a Voting Computational Routine, and a Failure Isolation Routine (Figure 70).

The Transient Failure Removal Routine applies iteration to iteration reasonableness criteria to the individual sensor readings, and removes any sensor that fails the criteria from the voting logic. If a sensor subsequently passes the reasonableness criteria it is reinstated as a candidate in the voting routine.

The Voting Computational Routine selects the best of the sensors which have not been declared temporarily or permanently failed and computes the orthogonal output data. The selection process of this routine is based upon a least squares best estimate of the error for each sensor.

The Failure Isolation Routine applies scale factor error/bias level criteria to each active sensor. If a sensor exceed the failure threshold level for a sufficient umber of iterations, that sensor is declared a permanent failure and is removed from further consideration by the RDM.

The accelerometer RDM and the gyro RDM utilize similar logic for their respective Transient Failure, Voting and Failure Isolation routines. the major difference between the gyro RDM and the accelerometer RDM are in the input axes cone angle/orientation and in the failure monitoring thresholds.

It is to be noted that failure monitoring thresholds and time delays for the RDM's are selected for the specific characteristics of the sensors, the aircraft, and the flight control system used for a particular application. The criteria and rationale for the threshold selection process is given in (ref. 23).

The signal selection subroutines in the DHS controls the sensory data which determines the "best estimate" for each parameter. Should a transient or permanent failure occur, the associated sensory data is not utilized in "best estimate" computations.

The final portion of the DHS is the output parameter computation which uses the best-estimate data to derive the output parameters listed in Table 11. To obtain optimum performance, parameters such as attitude, heading, local level velocities, and position are determined from a set of complementary filters as shown in Figure 71.

3. SYSTEM DEVELOPMENT STATUS

The varies ISS functions are being developed and evaluated individually and combined in building-block fashion into a total ISS. Following design/synthesis, the methodology utilized to perform the design verification for each function is similar in nature and includes analytic studies and laboratory test and evaluations.

The analytic studies consist of determing system performance capabilities and error sensitivities via computer simulation. In addition to determining the quality of the output parameters, a detailed evaluation of the RDM is also performed to assure that redundancy requirements can be met under such sensor failure conditions.

A block diagram of the digital simulation is shown in Figure 72. The simulation provides aircraft trajectory data, taking into account all six degrees of freedom. Different trajectories are generated by inputting pilot step commands into the flight control laws which, in turn, generates the surface commands. The surface commands are fed into the F-14 aerodynamic and structural models where skewed body rate and acceleration data containing body bending plus kinematic acceleration data are generated. Various sensor errors, such as bias and scale factor errors, are also introduced at this point in the simulation. The combined skewed sensory data is then fed into the ISS DHS where the RDM and best-estimate data computations are performed and orthogonal body rate and center of gravity body acceleration data are outputted. The open-loop switch shown in Figure 72 represents a software option. In the open-loop configuration, the control laws receive the required inertial data from the aerodynamic model; this allows evaluation of the ISS as a separate entity while exercising it in a realistic flying environment. In the closed-loop configuration, the ISS derived inertial data is utilized by the control laws to enable the designer to evaluae the ISS in a typical FCS design.

Integration of the ISS into the F-14 6-DOF simulation was accomplished to perform ISS evaluation. This system development/evaluation testing to data included:

- Failure threshold selection and testing.
- DHS parameter sensitivity studies e.g., cone angle, alignment, and c.g. location uncertainty.
- Performance with and without state estimator compensation.
- Performance after one and two induced sensor failures.

The significant results and conclusions obtained from the simulation tests are:

1. Introduction of various and multiple failure modes in the gyros and accelerometers were detected and did not cause significant transients in control system performance.

2. Introduction of sensor bias and scale factor errors up to the levels appropriate for flight control sensors did not cause any significant degradation in flight control system performance.

3. Closed loop tests without the state estimator resulted in unstable aircraft performance. The effectiveness of the state estimator in removing the rates caused by aircraft bending modes was demonstrated.

4. System sensitivity studies indicate that the DHS is tolerant to large misalignment errors (up to 0.2 DEG.) and large uncertainties in sensor to C.G. lever arm ($\pm$ 15%).

The ISS laboratory testing that followed the digital simulation effort was performed in Grumman's Fly-By-Wire Laboratory depicted in Figure 73. The aerodynamic and structural models of the aircraft are contained in an analog computer and used to drive the three-axis Flight Attitude Table (FAT). The ISS gyro and accelerometer arrays are mounted on the FAT (Figure 74) to provide inputs to the ISS DHS contained in the FBW Laboratory Digital Computer. An independent inertial reference assembly mounted on the FAT provides a three-axis orthogonal gyro and accelerometer data for comparison with ISS-derived data. The outputs from the ISS DHS are fed to control laws within the digital computer which, in turn, provide actuator commands to the aerodynamic model contained in the analog computer.

The laboratory test plan included open and close loop testing similar to the evaluation testing performed on the all-digital simulation. The emphasis in the laboratory testing was on the following areas:

- Verification of state estimator performance.
- Verification of failure isolation capability.
- Monitoring aircraft performance in the presence of induced sensor failures.

The results of laboratory testing clearly showed that the RDM could successfully provide high-quality two-fail operational gyro and accelerometer data for FCS applications in the presence of local body bending. In addition, accelerometer lever arm effects due to the dispersed sensor locations were determined and compensated in order to provide the aircraft with center of gravity body accelerations.

The significant results obtained from the laboratory testing are:

1. The state estimator design, modified for the laboratory test fixture, was effective in removing bending rates and kinematic accelerations.

2. First and second faiures of gyros and accelerometers were isolated with no observable transients in aircraft parameters.

Following the FCS skewed gyro/accelerometer development phase, a combined development effort for FCS and Attitude/Heading Reference system functions was initiated. The major differences between this system configuration versus the previous configuration are:

- Utilization of medium grade inertial instruments to provide dual FCS and AHRS functions.

- Redesign of the DHS to

  - Include a new state estimator to extract body bending/lever arm effects for the dual functions

  - Incorporate the algorithms for computing AHRS functions.

The associated digital simulation and laboratory test setup are similar to that previously described with the above modifications. The digital simulation/evaluation effort has been successfully completed; the results showed that both FCS and AHRS functions can be achieved with a common set of dispersed inertial instruments subjected to dissimilar flexible body bending. The laboratory hardware is currently being set up. It is functionally similar to that shown in Figure 73 but will utilize medium-grade inertial components (i.e., rate gyros with an accuracy of 10 degree/hour and accelerometer with an accuracy of 0.002g) and contains the DHS changes described above. Detailed performance testing is in process in the Grumman Fly-By-Wire Laboratory.

The air data system design effort for conventional takeoff and landing (CTOL) has been completed and the digital simulation effort is currently underway. A block diagram of the simulation is shown in Figure 75. In order to provide realistic parameters for the simulation, certain characteristics of the air data system fromthe F-14A flight test aircraft were utilized. For example, F-14A left/right and nose boom probe position error models are utilized within the DHS data normalization algorithms. Pneumatic lag models from the F-14A are also utilized. Actual F-14A flight test data, both steady state and maneuvering, are being utilized for generating the simulated pneumatic inputs.

In support of the system design effort, wind tunnel tests have been completed on both hemispherical-shaped (ref. 31) and aerodynamically compensated multi-purpose probes.

In preparation for a future combined ISS test program, the laboratory test facilities are currently being modified to include a triple channel of air data test equipment consisting of computer-controlled pneumatic function generators and secondary pressure standards as shown in Figure 76.

Future ISS development plans include development of a low airspeed omni-directional air data system to begin in Fall of 1982. In addition, a design effort utilizing advanced inertial sensors, such as strapdown two-degree-of-freedom rate integrating gyros, is in progress. Following these efforts, the navigation/landing guidance synthesis and laboratory test and evaluation of the air data system will be performed.

4. CONCLUSIONS

to comply with the flight control sensory requirements for future aircraft, it is clear that a new, innovative approach was necessary. A systems designer/integrator, such as Grumman, must examine all aspects including performance, reliability/maintainability, operational readiness, and life-cycle cost to be assured that the total system requirements are satisfied. At this point, it appears that our Integrated Sensory System approach offers the greatest potential to satisfy these system requirements when compared to the dedicated hardware approach utilized in current aircraft. These system requirements are literally translated to design objectives with this approach and include:

- Dual-fail operational characteristics where necessary.
- Maximum use of mature hardware to assure that reliability/ maintainability goals are achievable.
- Maximum use of standard modules to reduce life-cycle cost and assure procurement of competitive hardware.
- Built-in-test to permit rapid fault isolation and minimize I Level maintenance.
- Dispersed components to achieve a high degree of survivability.

The conclusions reached from the digital simulation and laboratory evaluation of the synthesized data handling system are:

1. The skewed inertial sensor concepts, which utilize six rate gyros and six accelerometers, can provide dual fail-op rate and acceleration data to DFBW flight control systems, as well as to other aircraft sub-systems.

2. It is feasible and practical for flight control application, using current digital computer technology, single degree-of-freedom gyros, and standard flight control system accelerometers, to perform skewed inertial sensor redundancy management with compensation for aircraft bending modes and kinematic acceleration effects.

3. A state estimation scheme required to perform the compensation for bending modes and kinematic accelerations was developed. The use of this compensation permits complete flexibility of sensor location for improved survivability and accessibility.

Finally, it is clear that our efforts to date have resulted in techniques and approaches to solve these problems. It is also apparent that the techniques require further development and evaluation. The logical development cycle planned will prove the techniques to be feasible and practical in meeting the needs of future aircraft. In closing, a summary of the ISS accomplishments to date are shown in Table 12.

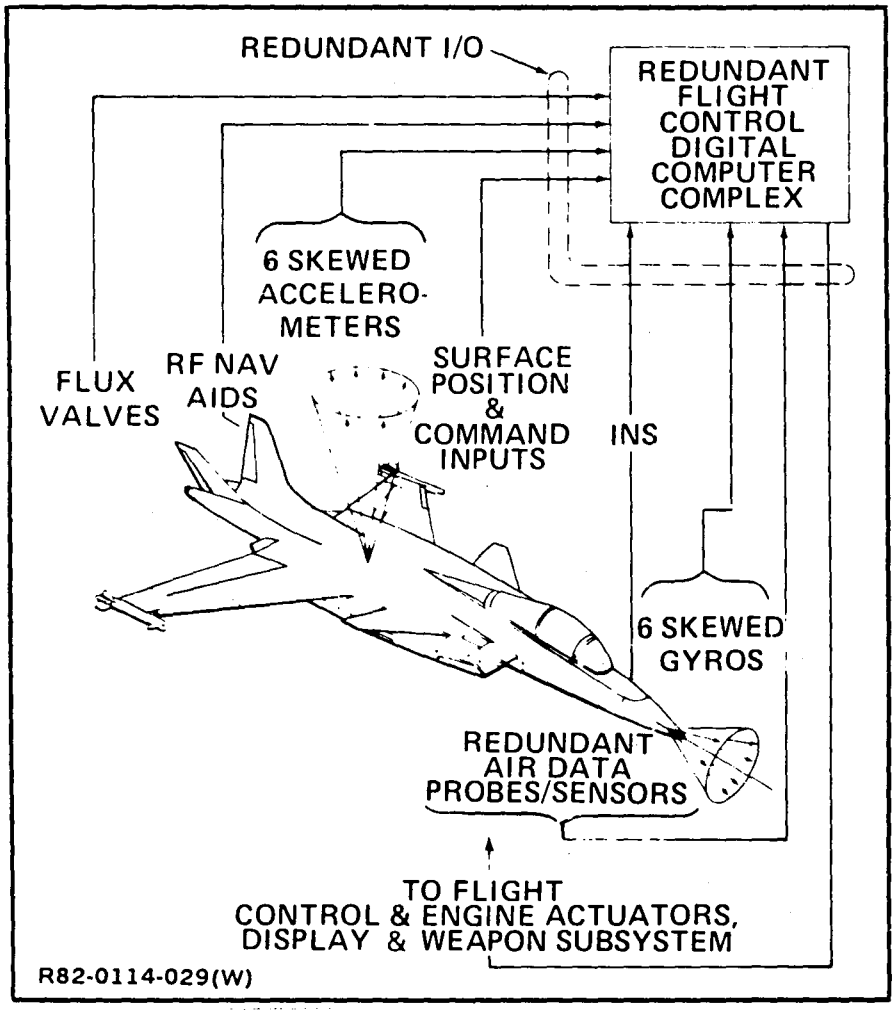


Figure 64 Integrated Sensory Subsystem

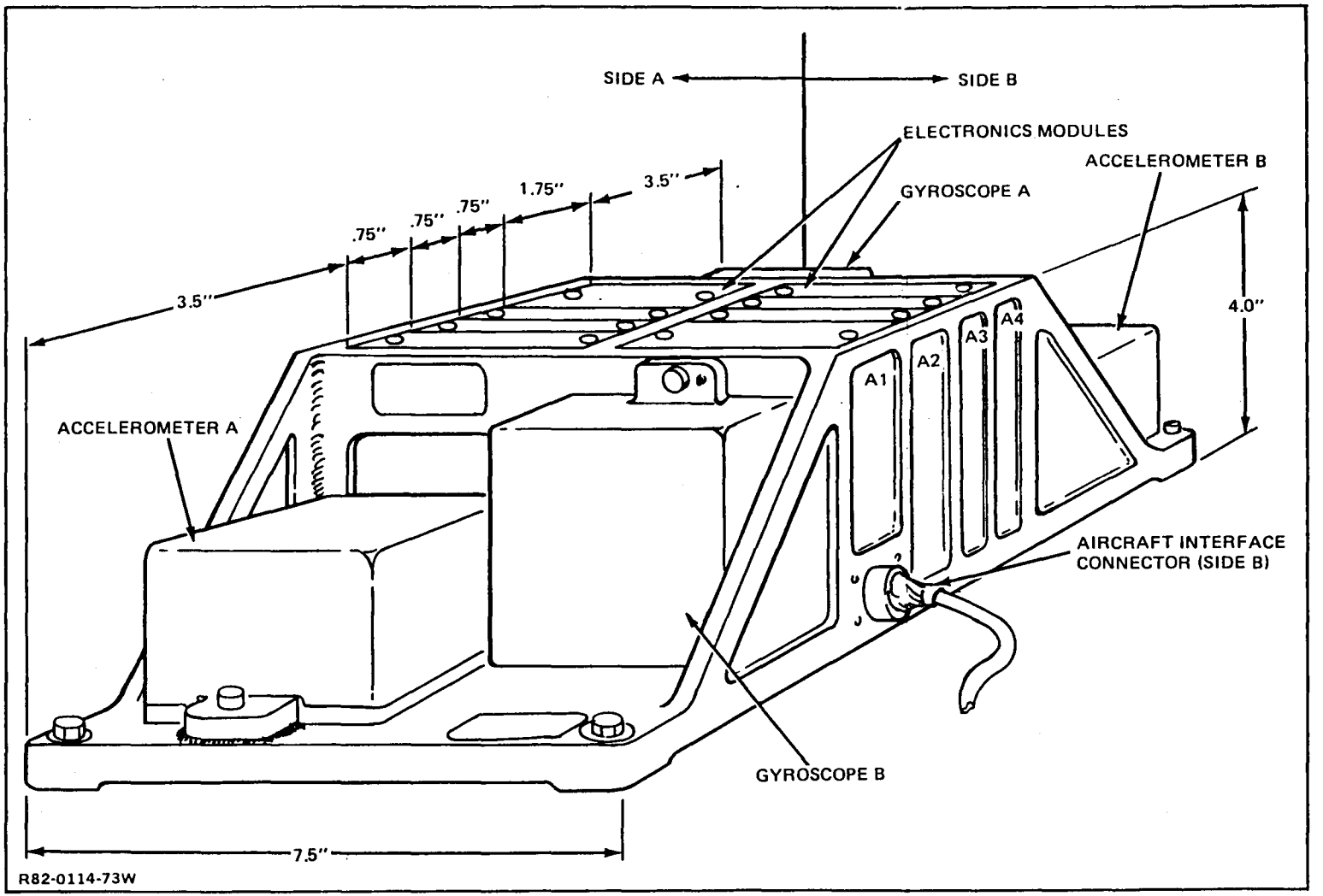


Figure 65 Inertial Component Assembly

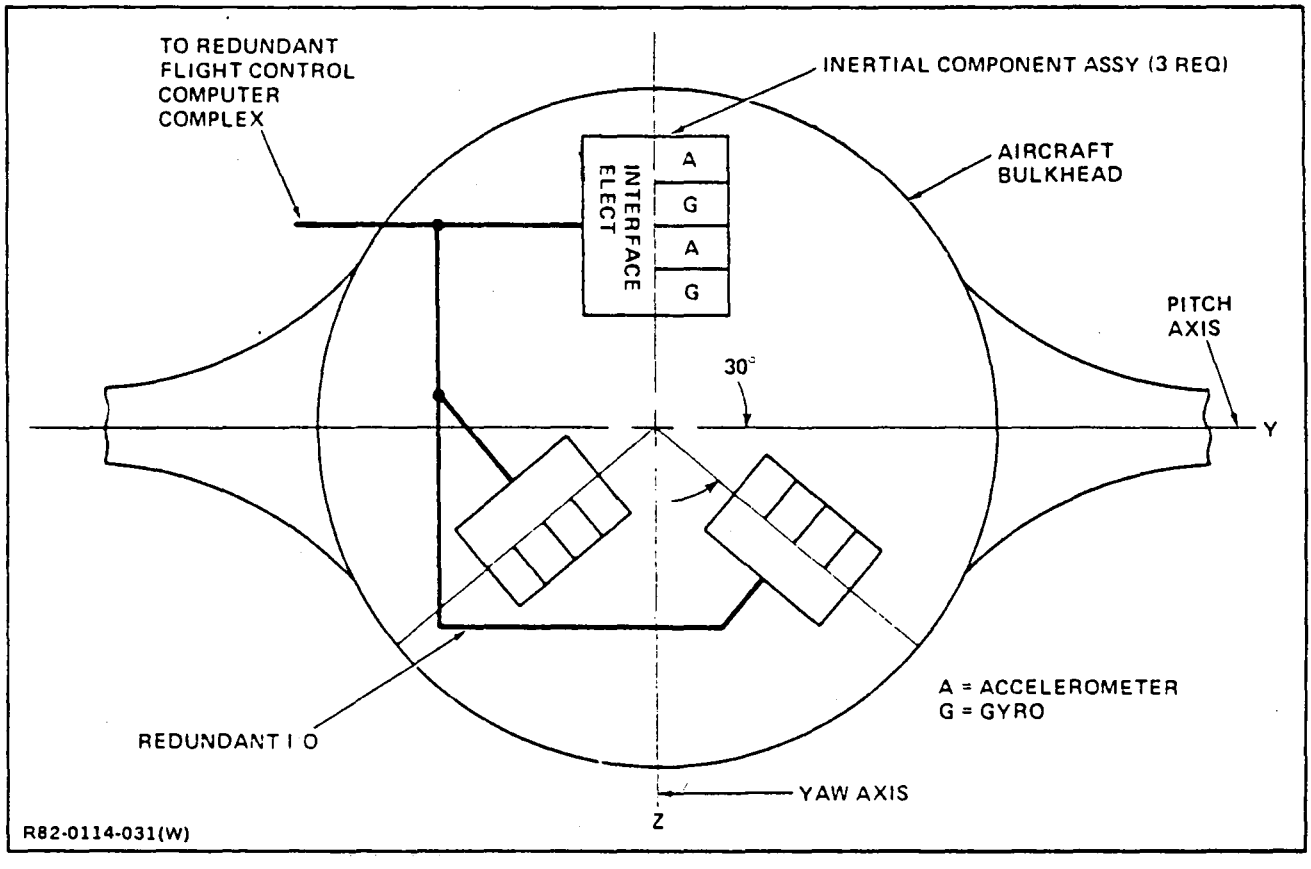


Figure 66 Inertial Subsystem Hardware Configuration

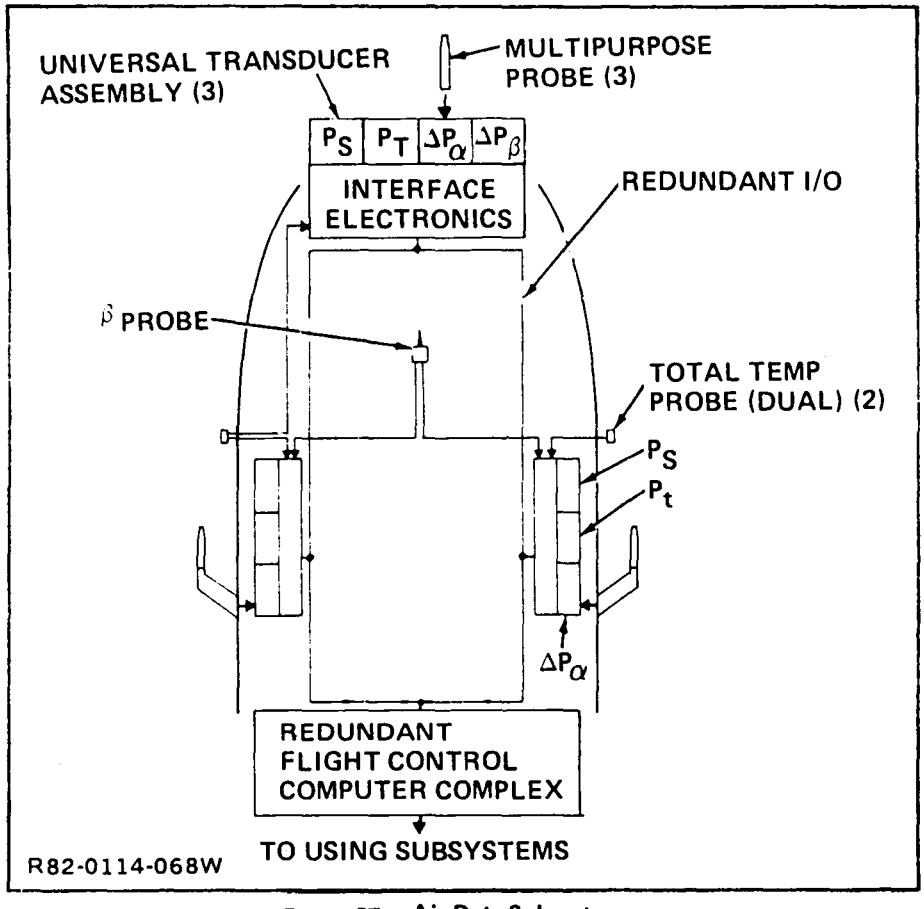


Figure 67 Air Data Subsystem

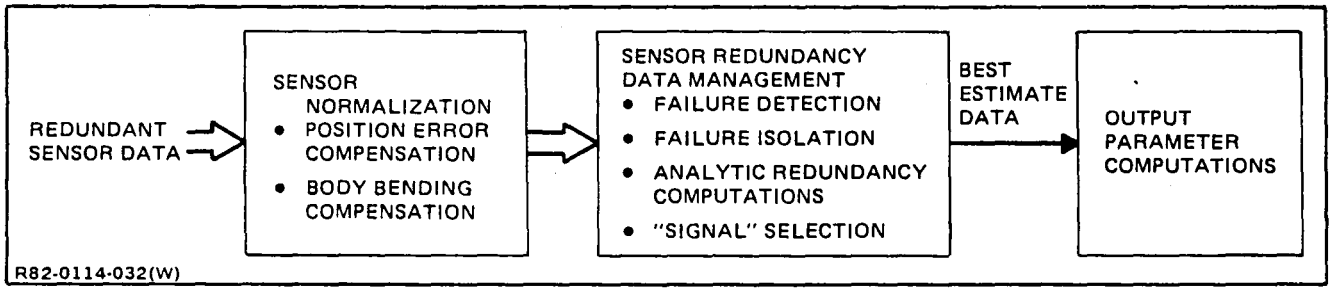


Figure 68 ISS DHS Block Diagram

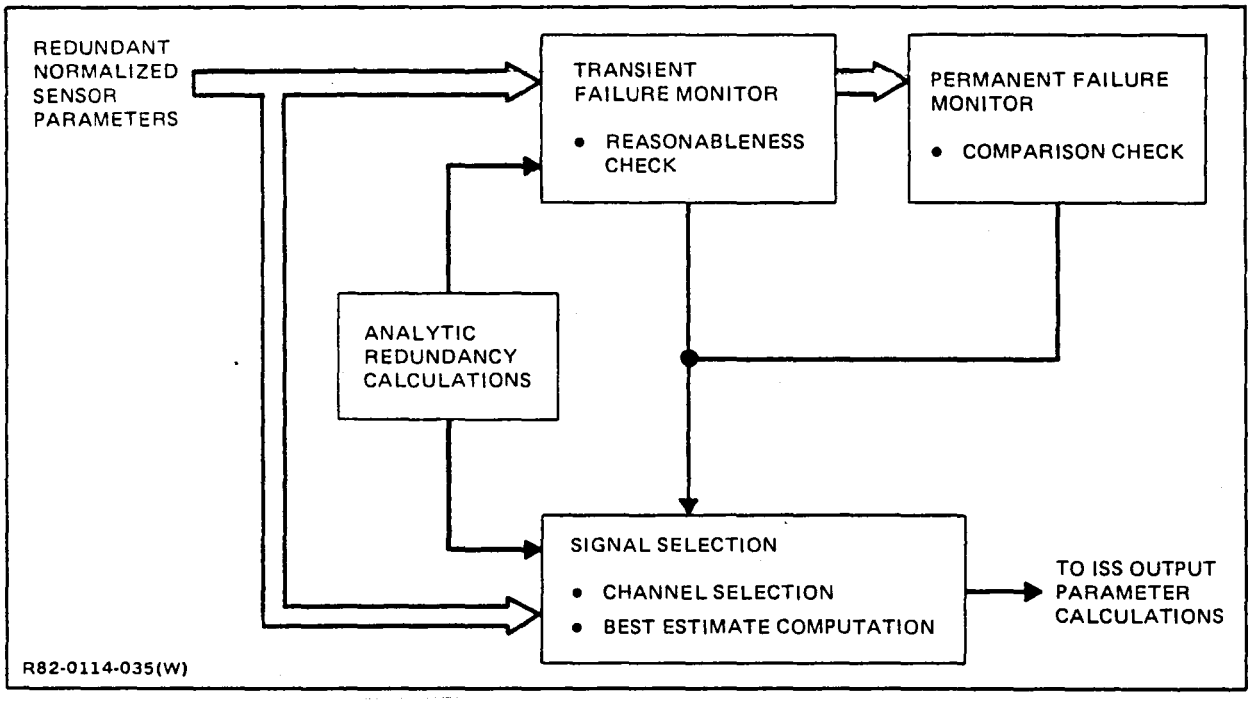


Figure 69 Redundancy Data Management

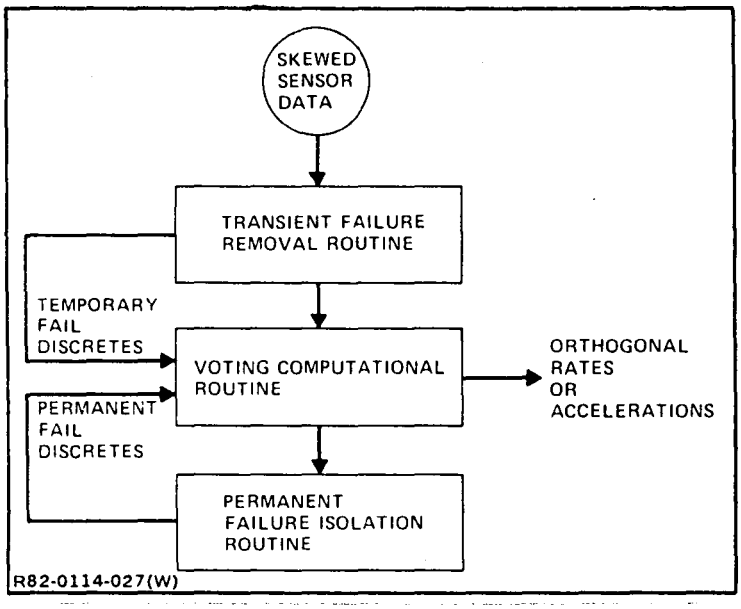


Figure 70 **Gyro or Accelerometer Redundancy Management**

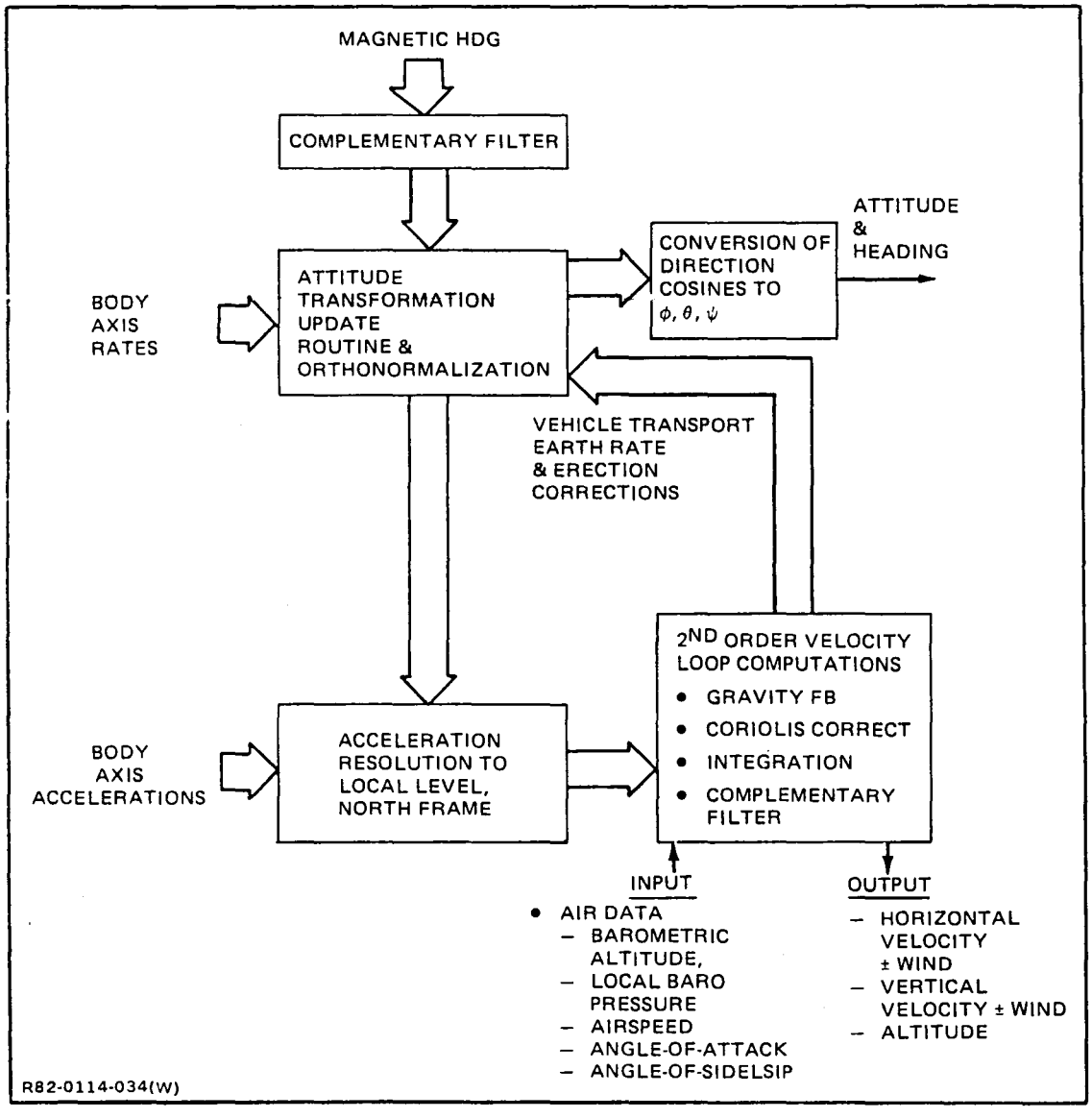


Figure 71 Attitude/Heading/Velocity Block Diagram

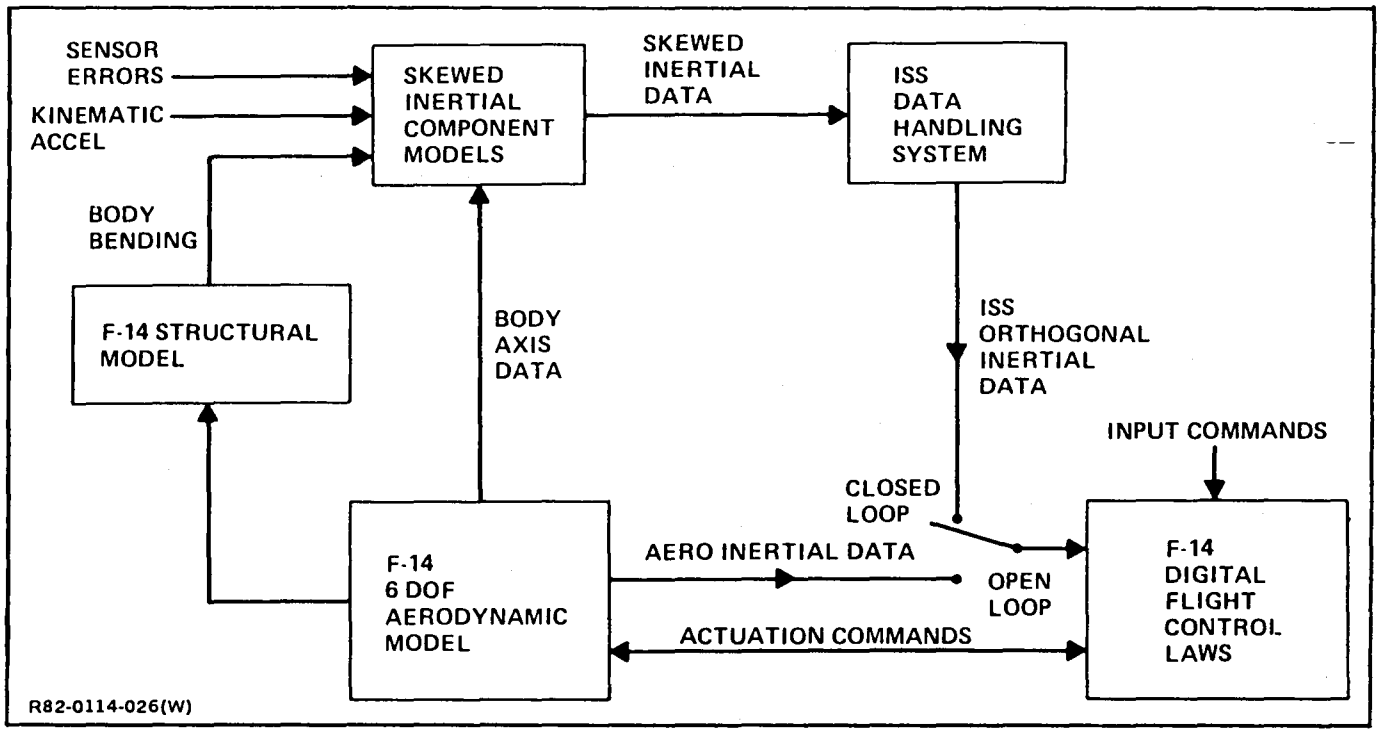


Figure 72 **ISS Digital Simulation Gyro/Accelerometer (FCS)**

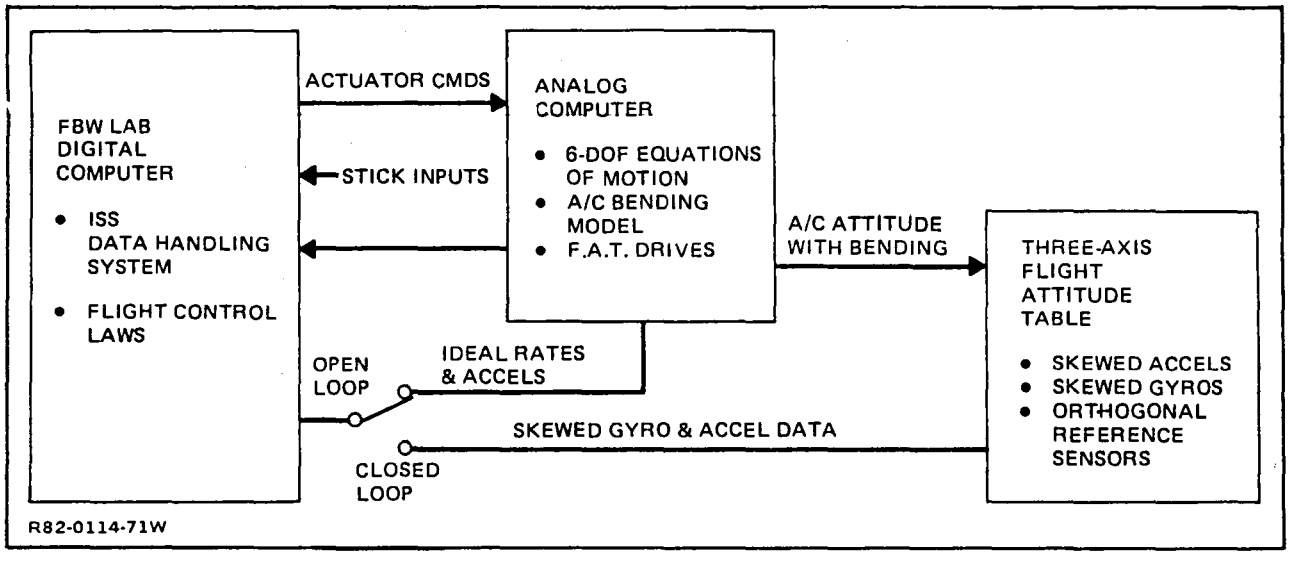


Figure 73 ISS Laboratory Hardware Test/Evaluation

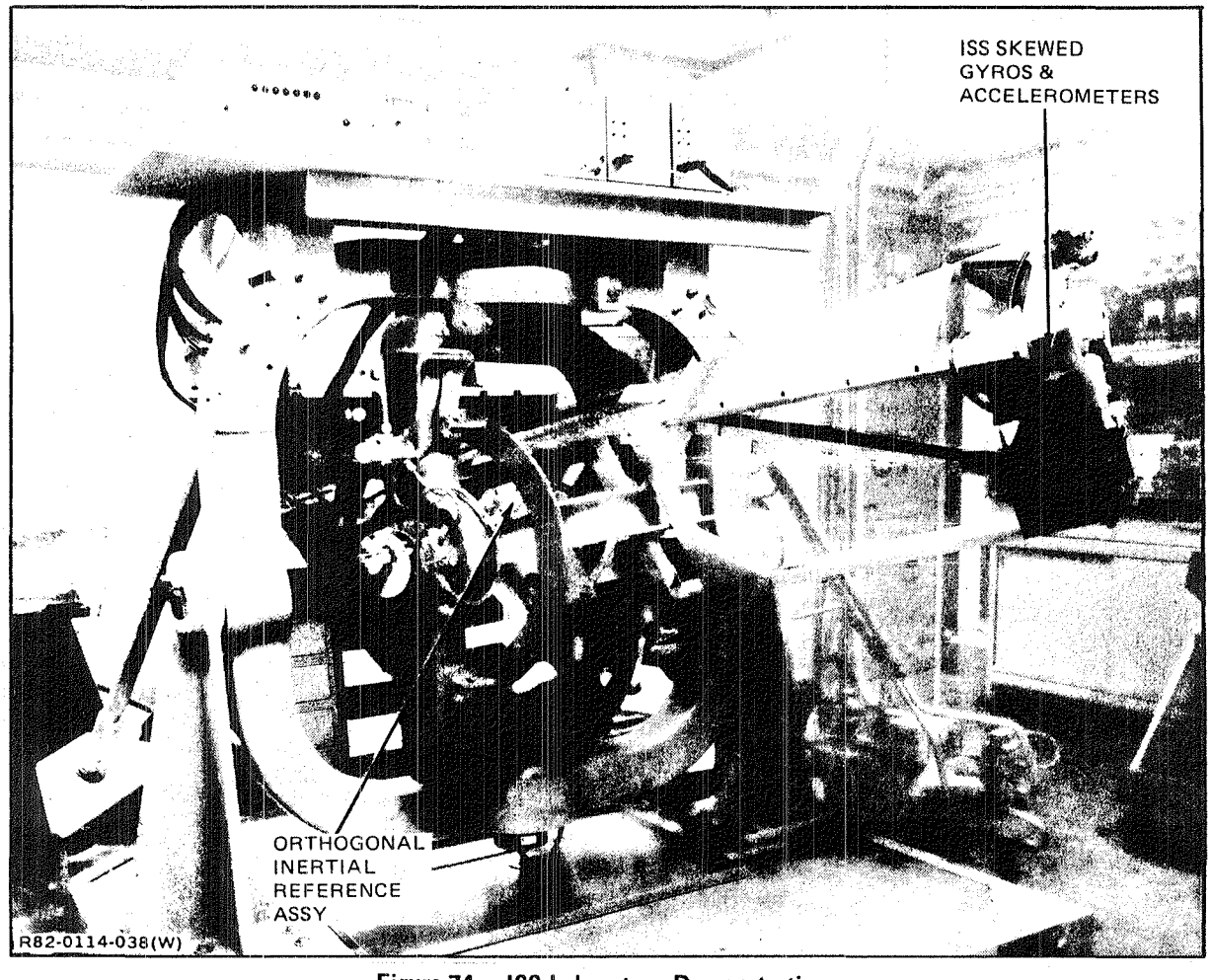


Figure 74 ISS Laboratory Demonstration

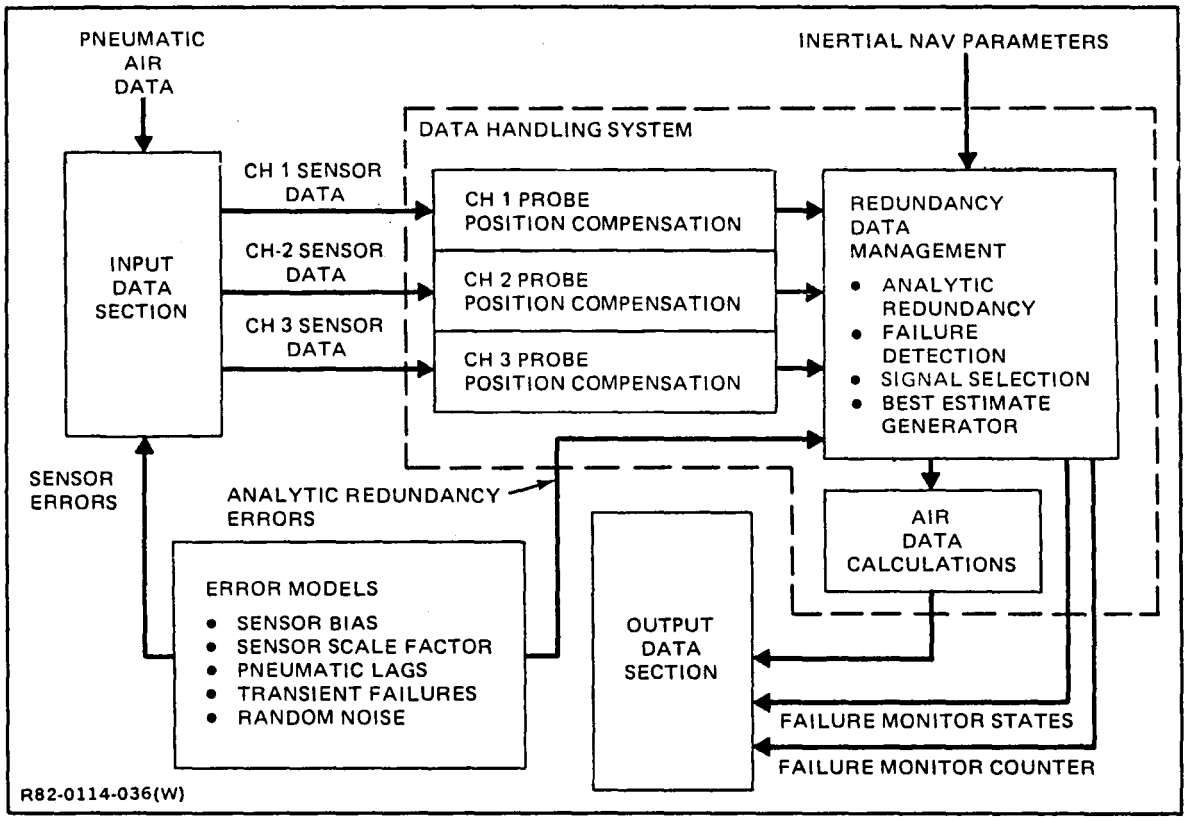


Figure 75 Air Data Simulation Block Diagram

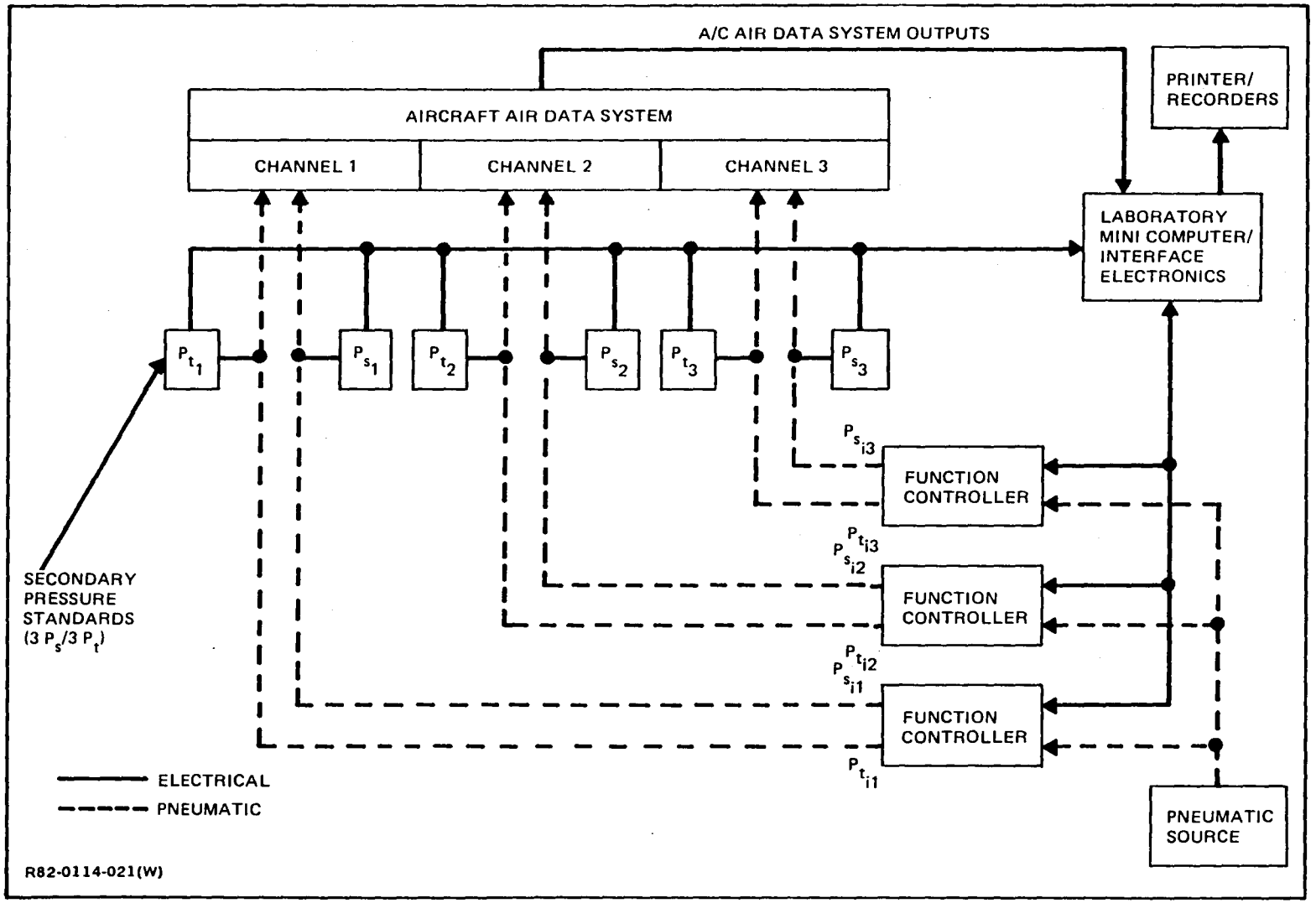


Figure 76 Air Data Laboratory Test Set-up

Table 11 ISS Output Parameters

- THREE-AXIS BODY RATES
- THREE-AXIS BODY ACCELERATIONS
- ATTITUDE/HEADING
- THREE-AXIS LOCAL LEVEL VELOCITIES
- LANDING/GUIDANCE RELATIVE NAV
- PRESSURE ALTITUDE
- AIRSPEED & MACH
- DYNAMIC PRESSURE
- ANGLE-OF-ATTACK
- ANGLE-OF-SIDESLIP
- RELATIVE WIND

R82-0114-033(W)

Table 12 ISS Accomplishments

- SKEWED/DISPERSED INERTIAL COMPONENTS FOR ADVANCED FLIGHT CONTROL SYSTEMS
  - FLIGHT TEST DEMONSTRATION ON RIGID BULKHEAD
  - LABORATORY TEST DEMONSTRATION WITH FLEXIBLE BODY BENDING
  - SIMULATION UTILIZING UPGRADED INERTIAL COMPONENTS TO PROVIDE AHRS FUNCTIONS
  - LABORATORY TEST DEMONSTRATION TO PROVIDE FCS & AHRS FUNCTIONS*
  - SIMULATION & LAB EVALUATION OF ADVANCED STATE-OF-THE-ART GYROS*
- DISPERSED AIR DATA SENSORS CONFIGURED FOR ADVANCED FLIGHT CONTROL SYSTEMS
  - WIND TUNNEL TESTS OF MULTI-PURPOSE PROBES
  - SIMULATION FOR EVALUATING SENSOR CONFIGURATION & DHS
  - LABORATORY TEST DEMONSTRATION OF REDUNDANT/DISPERSED AIR DATA COMPONENTS*

R82-0114-030(W) *IN PROCESS

APPENDIX E

REDUNDANT SENSOR CONFIGURATION DESIGN TRADEOFFS

1. Tradeoffs

Most discussions, analyses and designs involving redundant sensors reference spatial configurations wherein the orientation of the sensor axes are defined by,

A - A uniform distribution on the surface of a cone.

B - A uniform distribution on the surface of a cone plus one sensor on the cone axis.

C - Normals to the faces of the five regular polyhedra; Tetra-, Hexa-, Octa-, Dodeca-, and Icosa-hedron.

Dependent upon the number of sensors involved and the specific cone angle, these three categories have some overlap. In addition, highly specialized configurations not strictly described by A thru C above, have been devised. We choose to ignore specialized configurations because consideration of such systems at this point would add little to the determination of fundamental redundant sensor configuration tradeoff sensitivities.

Without any loss of generality, four of the five regular polyhedra can be represented by half of their faces above or below a plane of symmetry. In this case, an equivalent cone model may be formed with the cone vertex as the spatial center of the polyhedron and the cone axis normal to the plane of symmetry. With the appropriate cone angle, cone configurations A and/or B can be made equivalent to the regular polyhedra. These equivalences and corresponding cone half-angles are summarized in Table 13. Per Table 13 the Semi-Icosahedron requires the compounding of cone configurations A and B, while the remaining four regular polyhedra are uniquely equivalent to A or B. For our purposes, any subsequent requirement to analyze a 10 sensor configuration can be adequately represented by cone models A or B, so we will neglect the compound cone configuration of the Semi-Icosahedron henceforth.

In general, cone models A and B are sufficient to develop the significant tradeoff sensitivities involving any number of redundant sensors, including 4 of the 5 regular polyhedra where the appropriate cone angle is specified.

In terms of evaluating the performance of redundant sensor configuratoins, we ultimately need to consider how the individual sensor errors into the primary p, q, r A/C axes. The characteristics of this mapping must be evaluated for full sets of sensors and for the remaining partial sensor sets after failures have occurred.

Figure 77 highlights the basic error relationships associated with cone configuration models A and B. With a full set of n sensors, a value of cone half-angle β, can be selected to minimize the p, q, r error ellipsoid. The optimum cone half-angles are summarized below C in Figure 77. It is noted that the optimum cone half-angle in Figure 77 are identical to the cone half-angle designations in Table 13; the spatially uniform location of regular polyhedra faces is analogous to uniform sensor sensitivity in 3-dimensional space.

In addition, note that the optimum cone half-angle cone model A is a constant 54.74 degrees while the optimum angle for cone model B is a function of the number of sensors. The constant optimum cone half-angle characteristic of cone model A is particularly convenient because it simplifies the analysis of tradeoff situations involving various combinations of multiple and/or identical sensor subsets. Since the cone angle is not a function of , linear superposition applies, and "analytical cones" can be created by simple rotations of subsets as long as a colinear relationship between the cone axes is maintained. For example, a six-sensor cone can be created with 2 three-sensor cones (i.e., orthogonal triads) rotated 60^{o} with respect to each otehr about their cone axes, or equivalently, about the triad diagonals. The possible combinations are endless (e.g., a 12 from two 6's or four 3's, etc....), and they provide a fair amount of flexibility in the design of both software and hardware, including the possible utilization of proven sensor packages. The advantages cited for cone configuration A certainly do not preclude the viable implementation of a redundant sensor configuratoin per cone model B, but for the purposes of developing basic redundant sensor configuration tradeoff sensitivities, at least initially, the use of the cone A model is preferable.

The Fail-Op capability of redundant sensor configuratoins is a main design driver in terms of the probability of mission success and maintenance cycle parameters. Single sensor cones have a Fail-Op capability equal to N-4, where N equals the total number of sensors. (It requires a minimum of 5 sensors to detect and isolate a single failure.) One might consider cascading conventional orthogonal triads wherein the sensor axes are colinear. The Fail-Op capability of this configuration is $\frac{N}{3} - 2$. If cones are cascaded, the Fail-Op capability is given by $N - 4n_c$, where n_c is the number of identical cones. The Fail-Op capability vs. the total number of sensors for single cones, cascaded cones, the cascaded orthogonal triads is plotted in A of Figure 78.

In general, cascaded orthogonal triads have the poorest Fail-Op capability for a given number of sensors while the single cones have the best and cascaded cones fall somewhere between.

One might question the consideration of cascaded cones at all, since identical cascaded cones could be rotated to form "analytical or effective single cones" as mentioned previously - with a much improved Fail-Op capability. Significant justification exists however, for the consideration of cascaded cones in terms of related tradeoffs with respect to the corresponding computer and software configurations. For example, comparisons of the simultaneous failure detection and isolation of 18 sensors on a single cone (analytical or real) vs. parallel processing of 9 sensors in two cones or 6 sensors in 3 cones have to be analyzed in terms of failure modes, reliability, system interface and I/O characteristics, development costs, maintenance costs, ..., etc.

In addition, one could suggest that tradeoffs conducted to optimize the overall redundant sensor system design with respect to a given Fail-Op design goal might yield different results from the case where the Fail-Op capability was to be optimized given a limit on the maximum number of sensors. In short, this is a significant tradeoff area requiring a fair amount of detailed effort.

The allowable mean system error $\bar{\sigma}$, is another major design driver. As sensors fail, the mean system error will increase to some end-of-life value at the Fail-Op limit. This end-of-life error is a function of the initial number of sensors, the sensor quality, and the inherent failure degradation characteristic of the candidate redundant sensor configuration.

The initial value of the mean system error (i.e., with no failures) is not a function of the sensor configurations referenced in Figure 78 it is a function of the total number of sensors only. If the mean system error is normalized with respect to a common individual sensor error σ_S, we can refer to the relative mean system error, $\bar{\sigma}/\sigma_S$. the initial value of $\bar{\sigma}/\sigma_S$ as a function of total number of sensors is shown in B of Figure 78.

The degradation of $\bar{\sigma}/\sigma_S$ for two different redundant sensor configurations, each with a total of 24 sensors, is given in C of Figure 78. The performance of the 4 cascaded six-sensor cone configuratoin is based on a software simplification design policy of dropping each six-sensor cone off-line when it has reached its Fail-Op limit of 2 failures. The failure performance of this configuratoin is analyzed in the following section. On the other hand, the failure performance of the 8 cascaded triads was based on complete processing of all the remaining

sensors. No meaningful comparison between these two particular redundant sensor systems is intended or implied at this point. They were presented as examples to highlight another significant tradeoff area; the relationship between end-of-life performance and redundant sensor configuration.

In summary, it should be noted that this introduction to redundant sensor configuration tradeoffs is by no means comprehensive or complete. For example, practical considerations involving the use of non-optimum cone angles and the effect of different failure modes in certain classes of sensors (e.g., SDOF vs. TDOF gyros), are additional topics that may require further development - and there are no doubt, serveral more.

2. Relative Mean Error Relationships for Single and Cascaded Six Sensor Cones

In this section, the relative mean system error for cascaded six-sensor cones is developed as a function of the number of failed sensors and the individual sensor error variance.

We start by evaluating a single six-sensor cone as illustrated in Figure 79. The individual sensor axes s_1, thru s_6, are located on a cone of half-angle = β, with the cone axis coincident with one of the major A/C axes. The projections of the sensor axes in the plane of A/C axes q and r are symmetrically separated by an angle of 60^o.

It is noted that any computational processing of the six sensor outputs would have to account for the specific orientation of the cone with respect to the major A/C axes p, q, and r and the specific value of the cone angle as well. If the Figure 79 orientation represented a real implementation, then the transformation matrix H, in Figure 79 would of course have to be used in the actual processing. For the purposes of this appendix however, we use the specific H transformation in Figure 79 only as a convenient means of developing general results that are independent of any specific orientation.

The least mean squares solution for the A/C axes vector $\vec{A}$, is given by,

$$\vec{A} = [H^T H]^{-1} H^T \vec{S} \qquad (1)$$

where: $\vec{A} \triangleq [p\ q\ r\ ]^T$

$\vec{S} \triangleq [s, s_2\ s_3\ s_4\ s_5\ s_6\ ]^T$

If the vector errors in $\vec{A}$ and $\vec{S}$ are denoted $\delta\vec{A}$ and $\delta\vec{S}$ respectively, then from (1),

$$\delta\vec{A} = [H^T H]^{-1} H^T \vec{S} \tag{2}$$

It follows that the covariance matrices of the error vectors are related by,

$$\left\langle \delta\vec{A} \cdot \delta\vec{A}^T \right\rangle_{3x3} = [G]_{3x6} \left\langle \delta\vec{S} \cdot \delta\vec{S}^T \right\rangle_{6x6} [G^T]_{6x3} \tag{3}$$

where:

$$G \triangleq [H^T H]^{-1} H^T \tag{4}$$

$\langle \cdot \rangle \triangleq$ the statistical expectation operator

Now, if the individual sensors are similar, with a common zero mean Gaussian error variance of σ^2_s,

$$\left\langle \delta\vec{S} \cdot \delta\vec{S}^T \right\rangle = \underset{6x6}{[I]} \sigma_s^2 \tag{5}$$

.... and (3) may be expressed as,

$$\left\langle \delta\vec{A} \cdot \delta\vec{A}^T \right\rangle = [G \cdot G^T]\sigma^2_s \tag{6}$$

Usine (4),

$$G \cdot G^T = [H^T H]^{-1} \tag{7}$$

.... hence the A/C axes error covariance matrix per (6) may be finalized as,

$$\left\langle \delta\vec{A}^{2} \cdot \delta\vec{A}^{T} \right\rangle \triangleq \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{bmatrix} = [H^T H]^{-1} \sigma^2 s$$

where: $P_{11} = \sigma^2_p$ = p axis error variance

$P_{22} = \sigma^2_q$ = q axis error variance (8)

$P_{33} = \sigma^2_r$ = r axis error variance

$P_{ij} = P_{ji}$ = corresponding covariance terms for $i \neq j$ and i, j = 1, 2, and 3

It is convenient to normalize our results with respect to the individual sensor error variance and deal with the elements of $[H^T H]^{-1}$ only.

$$\text{e.g.,} \quad \frac{P_{11}}{\sigma^2_s} = \frac{\sigma^2_\mu}{\sigma^2_s} = [H^T H]^{-1}_{11} \text{ , etc...} \tag{9}$$

Using the H matrix of Figure E-3 the normalized error covariance matrix with all six sensors operating is given by (10).

$$[H^T H]^{-1} = \left[\begin{array}{c|c|c} \frac{1}{6\cos^2\beta} & 0 & 0 \\ \hline 0 & \frac{1}{3\sin^2\beta} & 0 \\ \hline 0 & 0 & \frac{1}{3\sin^2\beta} \end{array}\right] \tag{10}$$

Hence,

$$\frac{\sigma_p^2}{\sigma_s^2} = \frac{1}{6\cos^2\beta} \tag{11}$$

$$\frac{\sigma^2 q}{\sigma^2 s} = \frac{\hat{\sigma}^2 r}{\sigma^2 s} = \frac{1}{3\sin^2\beta} \tag{12}$$

If we wish to optimize the error covariance with six sensors operating, a value of β may be chosen that minimizes the trace in (10).

$$\text{TRACE} = \frac{\sigma_T^2}{\sigma_s^2} = \frac{\sigma_p^2 + \sigma_q^2 + \sigma_r^2}{\sigma_s^2} \tag{13}$$

then, using (11) and (12) in (13), the trace is given by,

$$\frac{\sigma_T^2}{\sigma_s^2} = \frac{1}{6}\left[\frac{1 + 3\cos^2\beta}{\sin^2\beta\cos^3\beta}\right] \tag{14}$$

Using (14), the solution to

$$\frac{d\left(\frac{\sigma_T^2}{\sigma_s^2}\right)}{d\beta} = 0$$

defines the optimum cone half-angle. The result is,

$$\beta = 54.74^{\circ} \tag{15}$$

....and

$$\left.\begin{aligned}\cos^2\beta &= \frac{1}{3}\\ \sin^2\beta &= \frac{2}{3}\end{aligned}\right\} \tag{16}$$

The 54.74 degrees cone half-angle per (15) is also the optimum angle for any number of sensors uniformly distributed around a cone. It is of interest to note that in the case of the six-sensor cone, the configuration with the optimum β is identical to two orthogonal triads rotated 60^{o} with respect to each other. For example, sensor subsets (s_1, s_3, s_5) and (s_2, s_4, s_6) in Figure 79 are orthogonal triads with their diagonals along the cone axis. Hence, any number of 6, 9, 12, etc...., sensor cones can be formed with appropriately oriented orthogonal triads.

If we use the optimum cone angle solution per (16) in (11) and (12), the result is equal relative variances,

$$\text{i.e.,} \quad \frac{\sigma_p^2}{\sigma_s^2} = \frac{\sigma^2 q}{\sigma^2 s} = \frac{\sigma^2 r}{\sigma^2 s} = \frac{1}{2} \tag{17}$$

Since the normalized trace is not a function of the specific H matrix involved, we can state that

$$\frac{\sigma_T^2}{\sigma_s^2} = \frac{\sigma_p^2 + \sigma_q^2 + \sigma_r^2}{\sigma_s^2} = \begin{cases} \dfrac{1}{6} \quad \dfrac{1 + 3\cos^2\beta}{\sin^2\beta \cos^2\beta} & \text{; for general } \beta \\ \dfrac{3}{2} & \text{; for optimum } \beta = 54.74^{o} \end{cases} \tag{18, 19}$$

....for any orientation of the cone with respect to the p, q, and r A/C axes and with six sensors operating.

At this point, we would like to express the relative error in some mean sense that is convenient; arithmetic, geometric, or harmonic mean. Since the sum of the individual variances is the invariant combination, the arithmetic mean is both convenient and the most conservative. Let the normalized arithmetic mean variance be represented as $\bar{\sigma}^2/\sigma^2{}_s$, where,

$$\frac{\bar{\sigma}^2}{\sigma_s^2} = \frac{1}{3}\left[\frac{\sigma_p^2 + \sigma_q{}^2 + \sigma_r{}^2}{\sigma_s{}^2}\right] = \frac{1}{3}\left[\frac{\sigma_T{}^2}{\sigma_s{}^2}\right] \tag{20}$$

Then, for (18) and (19) in (20), we may summarize the basic results thus far as,

$$\left.\begin{array}{l}\text{Relative Mean}\\ \text{Error For}\\ \text{Six-Sensor Cone}\end{array}\right\} \triangleq \frac{\bar{\sigma}^2}{\sigma_s^2} \begin{cases} \frac{1}{18}\left[\frac{1+3\cos^2\beta}{\sin^2\beta\cos^2\beta}\right] & ;\ \text{for general } \beta \quad (21) \\ \frac{1}{2} & ;\ \text{for optimum } \beta = 54.74^o \quad (22) \end{cases}$$

Since a six-sensor cone has a Fail-Op = 2 capability, we must develop the relative mean error for the additional cases of one and two sensor failures. We will continue the development in terms of a general cone half-angle β, since it is not necessarily true that the optimum cone angle for 6 out of 6 sensors operating, is the same as the optimum cone angle for 5 out of 6 and/or 4 out of 6 sensors operating. Non-optimum cone angles in redundant sensor configurations can be utilized for the purpose of maximizing end-of-life performance by trading off initial mean error with all sensors operating vs. end-of-life mean error at the Fail-Op limit.

To represent a single sensor failure, we can delete any row of the matrix of Figure A1 and proceed to compute $[H^TH]^{-1}$ as before. The result is,

$$\left(\frac{\sigma_T^2}{\sigma_s^2}\right)_{5/6} = \frac{2}{9}\left[\frac{1+3\cos^2\beta}{\sin^2\beta\cdot\cos^2\beta}\right] \quad (22)$$

.....where the subscript "5/6" is used to denote "5 out of 6 sensors operating".

Note that the β dependent term in (23) is identical to the β dependent term in (14). Hence, the optimum cone half-angles for 6 out of 6 sensors and 5 out of 6 sensors are identical; $\beta = 54.74$ degrees.

Then, using the definition of the arithmetic mean variance per (20) along with (23), yields,

$$\left(\frac{\sigma^2}{\sigma_s^2}\right)_{5/6} = \begin{cases} \frac{3}{27}\left[\frac{1 + 3\cos^2\beta}{\sin^2\beta \cdot \cos^2\beta}\right] & ; \text{ for general } \beta \\ \frac{2}{3} & ; \text{ for optimum } \beta = 54.74^o \end{cases} \tag{24}$$

Next, we consider a second sensor failure. For any two failures in the six-sensor cone, the normalized trace of $[H^TH]^{-1}$ is still invariant as long as the separation angle between the failed sensors is constant. Therefore, we must consider three distinct second failure modes; separation angles between the two failed sensors of 60^o, 120^o, and 180^o. Deleting two rows of the H matrix per Figure 79 with the three possible separation angles (e.g., s_1, and s_3 for a separation angle of 120^o), and computing $[H^TH]^{-1}$ as before, yields the following results.

$$\left(\frac{\sigma_T^2}{\sigma_s^2}\right)^{60^o}_{4/6} = \frac{15 + 37\cos^2\beta}{30\sin^2\beta \cdot \cos^2\beta} \tag{25}$$

$$\left(\frac{\sigma_T^2}{\sigma_s^2}\right)^{120^o}_{4/6} = \frac{5}{18}\left[\frac{1 + 3\cos^2\beta}{\sin^2\beta \cdot \cos^2\beta}\right] \tag{26}$$

$$\left(\frac{\sigma_T^2}{\sigma_s^2}\right)^{180^o}_{4/6} = \frac{3 + 13\cos^2\beta}{12\sin^2\beta \cdot \cos^2\beta} \tag{27}$$

....where the superscript angle notation represents the separation angle between the two failed sensors.

After the first sensor failure, it is clear from the geometry in Figure 79 that the probability of a separation angle of 180 degrees with the second sensor failure is one chance in five; 1/5. Similarly, the probability of a separation angle between two failed sensors of 60 degrees and 120 degrees is the same; 2/5. Therefore, the appropriate combination of the results in (25) thru (27) can be formed with a weighted arithmetic mean format, where the weighting is equivalent to the probabilities of occurrence as discussed above and shown in (28) and (29) below.

$$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{4/6} = \frac{1}{3}\left[\frac{2}{5}\left(\frac{\sigma_T^2}{\sigma_s^2}\right)_{4/6}^{60^0} + \frac{2}{5}\left(\frac{\sigma_T^2}{\sigma_s^2}\right)_{4/6}^{120^0} + \frac{1}{5}\left(\frac{\sigma_T^2}{\sigma_s^2}\right)_{4/6}^{180^0}\right] \quad (28)$$

After combining terms, the final result is,

$$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{4/6} = \frac{325 + 939\cos^2\beta}{2700\sin^2\beta \cdot \cos^2\beta} \quad (29)$$

If we compute the optimum cone half-angle as the solution to,

$$\frac{d\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{4/6}}{d\beta} = 0 \quad (30)$$

the result is $\beta = 54.55$ degrees for the 4 out of 6 sensor case. The value for 6 out of 6 and 5 out of 6 was previously computed as $\beta = 54.74$ degrees. The small difference of 0.19^0 in the β values is negligible and affects the (σ^2/σ_s^2) 4/6 value in the 4th decimal place. Therefore, for a six-sensor cone, the optimum cone half-angle in terms of minimizing the relative mean error for 0, 1, and 2 sensor failures is $\beta = 54.74$ degrees - for all practical purposes. The basic error relationships developed to this point are summarized in Table 14.

Before proceeding with the development of the relative mean system error for cascaded six-sensor cones, we must precisely define "cascaded". In the context herein, "cascaded" means replication of the basic six-sensor cone without any change in orientation.

One could define a configuration of six-sensor cones in which the cone axes are parallel, but where each successive cone is rotated to obtain uniform distribution of the sensors. For example, if 3 six-sensor cones are rotated about their axes exactly 20^{o} with respect to each other, the result would be analytically equivalent to a single 18-sensor cone; this is not what we are considering herein.

In addition, the specific implementation or utilization of the cascaded cone outputs must be defined in order to develop the approprite relative mean system error. First, it is assumed that the sensor Failure Detection and Isolation (FDI) software is replicated on a cone-by-cone basis; each six-sensor cone has a Fail-Op = 2 capability and the entire cone is dropped from the system after two failures are detected. Secondly, it is assumed that the p, q, and r axes outputs from each cone sub-system are approximately weighted to develop the final or system p, q, r values.

Summarizing the ground rules/definitions above, the following development of the relative mean system error for the cascaded six-sensor cone configuration is in accordance with (i) thru (iii) below.

(i) Simple replication of the basic six-sensor cone - total system Fail-Op capability = twice the number of cones.

(ii) Simple replication of FDI software - detection of two failures drops entire cone off-line.

(iii) System output is based on weighted combinations of individual cone sub-systems; cones with single sensor failures would be weighted less heavily than cones with no sensor failures.

With respect to (iii) above, the specific weighted combination used is the inverse of reciprocal sums. For six-sensor cones denoted 1, 2, 3, etc... in cascade, the relative mean system error is computed as,

$$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{SYSTEM} \triangleq \left[1 \Big/ \left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_1 + 1 \Big/ \left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_2 + 1 \Big/ \left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_3 + \ldots\right]^{-1} \qquad (31)$$

As an example, if the "system" was defined as 4 six-sensor cones in cascade, and one of the cones has a single failure, the relative mean system error would be computed in accordance with (31) as,

$$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{SYSTEM} = \left[1\Big/\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{5/6} + 1\Big/\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{6/6} + 1\Big/\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{6/6} + 1\Big/\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{6/6}\right]^{-1} \quad (32)$$

Then using, $(\bar{\sigma}^2/\sigma_s^2)_{5/6} = 2/3$

and $(\bar{\sigma}^2/\sigma_s^2)_{6/6} = 1/2$ from Table 14, the numerical value in (32) is,

$$\left(\frac{\sigma^2}{\sigma_s^2}\right)_{SYSTEM} = \frac{2}{15}$$

Next, we must consider the effect of sensor failure location and sequence. The variation of the relative mean system error vs. the number of failed sensors is not unique, except at the initial and end-of-life points.

i.e., $\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{\substack{SYSTEM \\ (INITIAL)}} = \frac{1}{2 \times (\text{NUMBER OF CONES})}$ for no failures

$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{\substack{SYSTEM \\ (END\text{-}OF\text{-}LIFE)}} = \left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{4/6} = 1.0312$ at the Fail-Op limit with two failures in the last on-line cone

If the faiures were to sequence throughout the system in a uniform manner (i.e., no second failure in one cone until all cones had at least one failure), the variation in relative mean system error would be optimum in the sense of maintaining the smallest error vs. the total number of failed sensors. On the other hand if the first two failures occurred in a single ocne and the next two failures occurred in another cone, and so on, the variation in relative mean system error would represent a worst case condition. It is this latter or worst case failure mode sequence we choose to present herein.

In addition to being conservative, tabulation of the worst case failure mode is convenient in terms of representing all results for different numbers of cascaded cones below some specified maximum with a single calculation set. For example, if it is concluded that 5 six-sensor cones in cascade is the maximum size system being considered, once the relative mean system errors are computed for each sensor failure upt to the Fail-Op limit, the results for 4, 3, 2, and 1 six-sensor cone systems are already included as subsets of the original 5 six-sensor cone system calculations.

This "one-shot" calculation set for 1 to 5 six-sensor cones in cascade is tabulated in Table 15 and plotted in Figure 80. The results in Table 15 are based on the optimum cone half-angle; 54.74 degrees, the single six-sensor cone relationships in Table 14 and the weighted combination of cone errors per equation (31).

It is noted that the relative mean system error is double-valued at sensor failure totals of 2, 4, 6 and 8 for the purpose of "constructing" Table 15 and clearly identifying the points where each cone goes off-line.

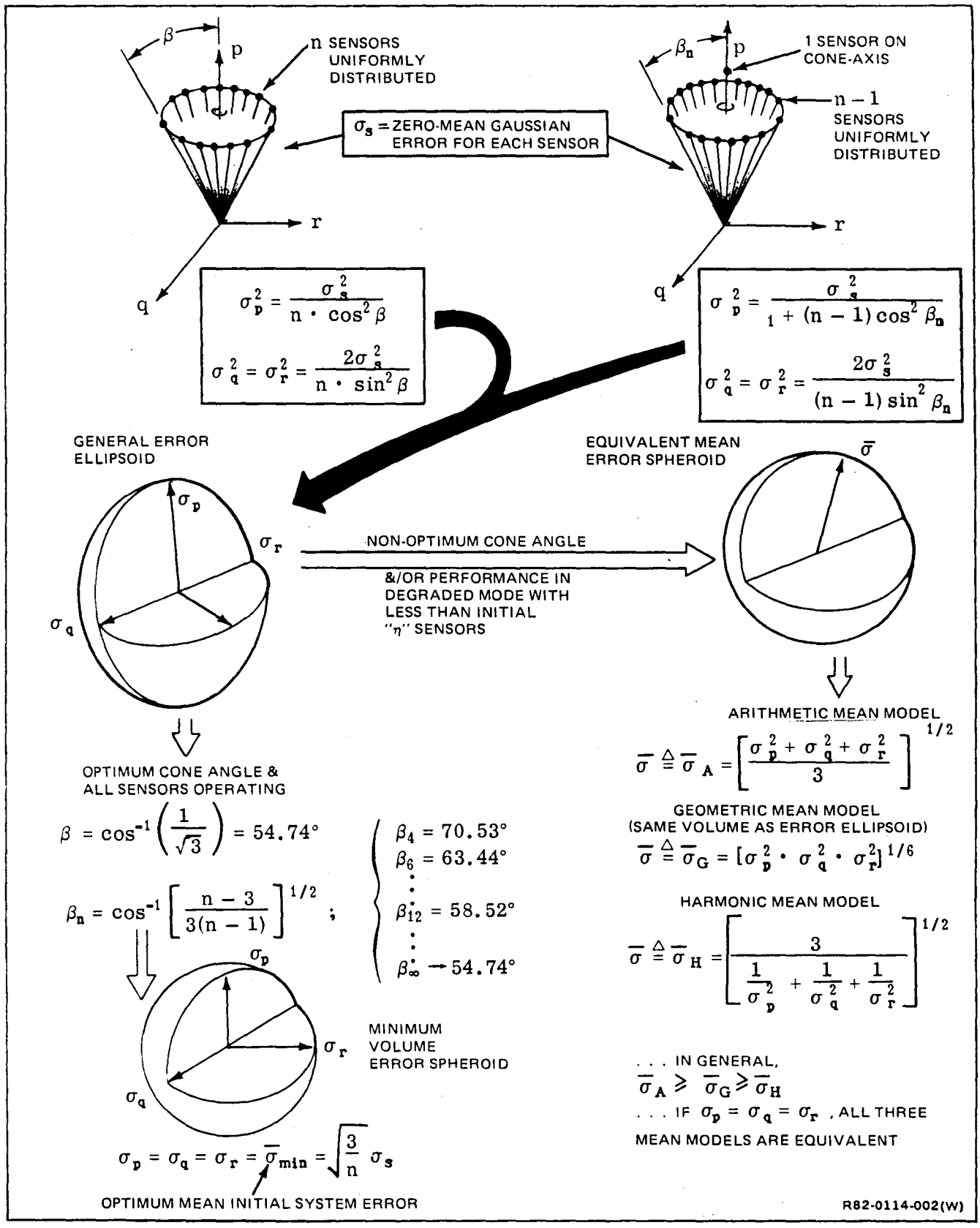


Figure 77 Redundant Skewed Sensor Error Geometry

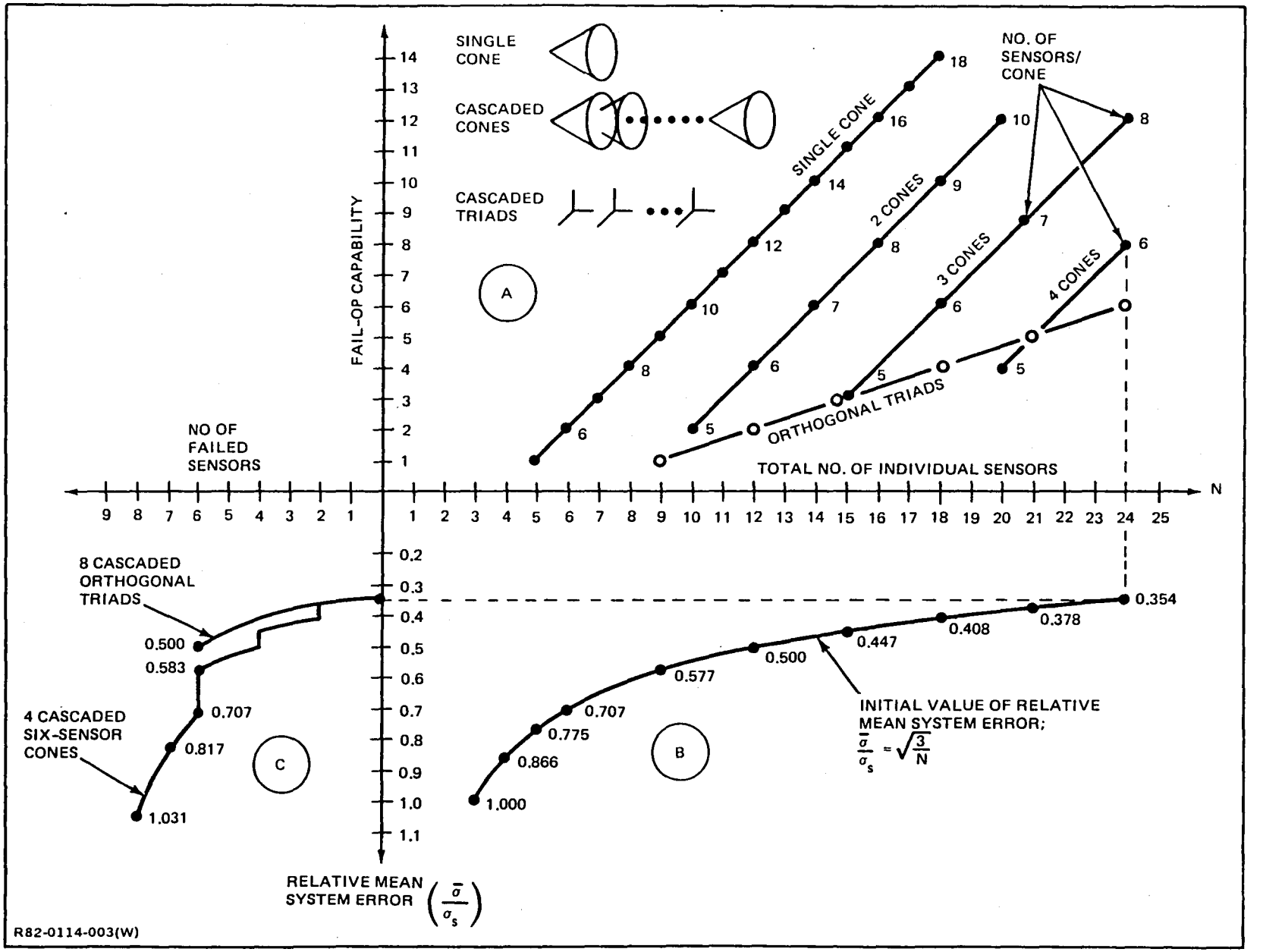
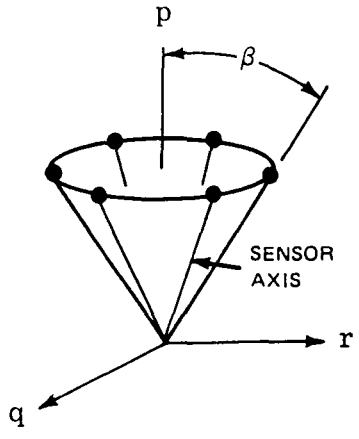
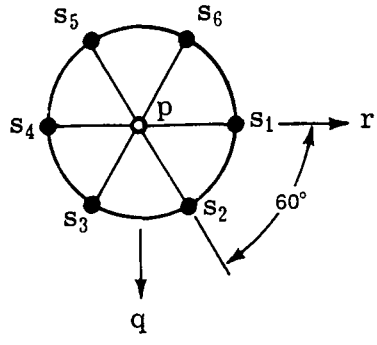


Figure 78 Redundant Sensor Configuration Tradeoffs



PROJECTION OF SENSOR AXES IN q – r PLANE



TRANSFORMATION FOR A/C TO SENSOR AXIS

$$\vec{S} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \end{bmatrix} = \underbrace{\begin{bmatrix} \cos\beta & 0 & \sin\beta \\ \cos\beta & \frac{\sqrt{3}\sin\beta}{2} & \frac{\sin\beta}{2} \\ \cos\beta & \frac{\sqrt{3}\sin\beta}{2} & -\frac{\sin\beta}{2} \\ \cos\beta & 0 & -\sin\beta \\ \cos\beta & \frac{-\sqrt{3}\sin\beta}{2} & -\frac{\sin\beta}{2} \\ \cos\beta & \frac{-\sqrt{3}\sin\beta}{2} & \frac{\sin\beta}{2} \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} p \\ q \\ r \end{bmatrix}}_{\vec{A}}$$

AIRCRAFT AXES

LEAST MEAN SQUARES SOLUTION FOR A/C AXES

$$\vec{A} = [H^T H]^{-1} H^T \vec{S}$$

ERROR COVARIANCE MATRIX

$$P \triangleq \langle \delta\vec{A} \cdot \delta\vec{A}^T \rangle = [H^T H]^{-1} \sigma_s^2$$

WHERE:

$P_{11} = \sigma_p^2 =$ p-axis ERROR VARIANCE

$P_{22} = \sigma_q^2 =$ q-axis ERROR VARIANCE

$P_{33} = \sigma_r^2 =$ r-axis ERROR VARIANCE

$\sigma_s^2 =$ INDIVIDUAL SENSOR ERROR VARIANCE

R82-0114-004(W)

Figure 79 Six-Sensor Cone Geometry

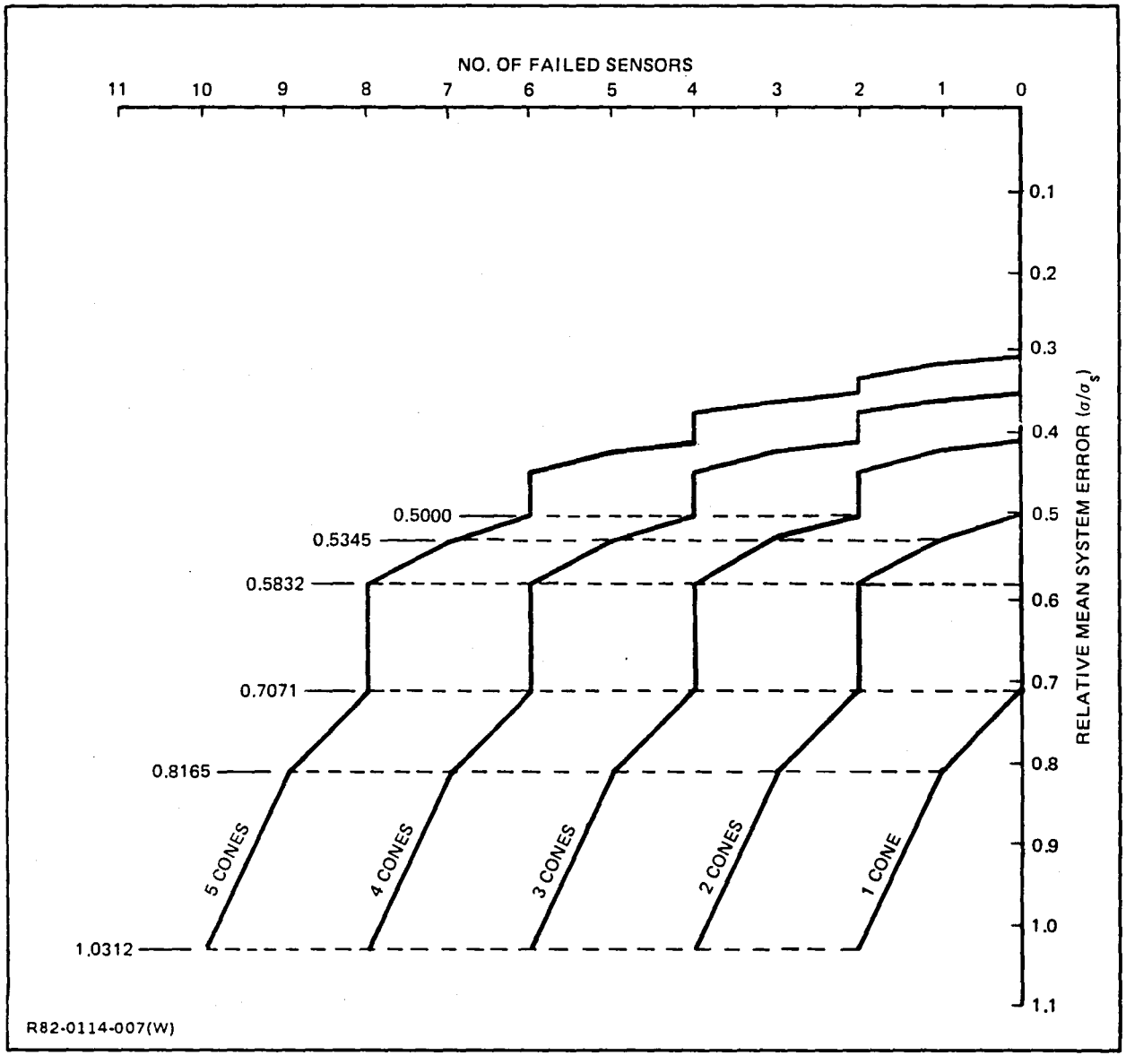
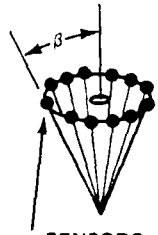
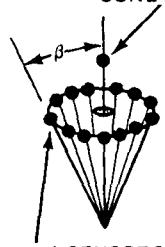
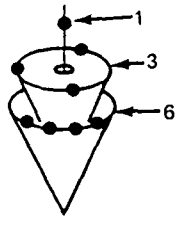


Figure 80 **Relative Mean system Error for Cascaded Six-Sensor Cones**

Table 13 Regular Polyhedra & Conical Equivalences in Redundant Sensor Systems

TOTAL NUMBER OF INDIVIDUAL SENSORS (n)	(A) 	(B) 	EQUIVALENT REGULAR POLYHEDRA
3	$\beta = 54.74°$		SEMI-HEXAHEDRON (CUBE) OR ORTHOGONAL TRIAD
4	$\beta = 54.74°$		SEMI-OCTAHEDRON*
4		$\beta = 70.53°$	TETRAHEDRON
6		$\beta = 63.44°$	SEMI-DODECAHEDRON
10	 COMPOUND CONES $\beta_3 = 37.3°$ $\beta_6 = 79.1°$		SEMI-ICOSAHEDRON**

*OFTEN REFERENCED WITH RESPECT TO TDOF GYRO IMPLEMENTATIONS
**SUITED FOR RING LASER GYROS & ACCELEROMETERS BECAUSE OF ICOSAHEDRON'S TRIANGULAR FACES

R82-0114-001W

Table 14 Relative Mean Error Relationships for a Single Six-Sensor Cone

NO. OF FAILED SENSORS	RELATIVE MEAN ERROR RELATIONSHIPS		
	$\frac{\bar{\sigma}^2}{\sigma_s^2}$		$\frac{\bar{\sigma}}{\sigma_s}$
	GENERAL β	OPTIMUM CONE HALF-ANGLE; $\beta = 54.74°$	
0	$\frac{1}{18}\left[\frac{1+3\cos^2\beta}{\sin^2\beta\cos^2\beta}\right]$	$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{6/6} = \frac{1}{2}$	$\left(\frac{\bar{\sigma}}{\sigma_s}\right)_{6/6} = 0.7071$
1	$\frac{2}{27}\left[\frac{1+3\cos^2\beta}{\sin^2\beta\cos^2\beta}\right]$	$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{5/6} = \frac{2}{3}$	$\left(\frac{\bar{\sigma}}{\sigma_s}\right)_{5/6} = 0.8165$
2	$\frac{325+939\cos^2\beta}{2700\sin^2\beta\cos^2\beta}$	$\left(\frac{\bar{\sigma}^2}{\sigma_s^2}\right)_{4/6} = \frac{319}{300}$	$\left(\frac{\bar{\sigma}}{\sigma_s}\right)_{4/6} = 1.0312$
R82-0114-005(W)	$\bar{\sigma}^2$ = MEAN SYSTEM (CONE) ERROR VARIANCE σ_s^2 = INDIVIDUAL SENSOR ERROR VARIANCE		

Table 15 Tabulated Values of Relative Mean Errors for Systems with 1 to 5 Six-Sensor Cones in Cascade

NO. OF FAILED SENSORS IN SYSTEM					NO. OF OPERATING SENSORS IN EACH CONE					*RELATIVE MEAN SYSTEM ERROR	
1 CONE SYSTEM	2 CONE SYSTEM	3 CONE SYSTEM	4 CONE SYSTEM	5 CONE SYSTEM	CONE 1	CONE 2	CONE 3	CONE 4	CONE 5	$\frac{\sigma^2}{\sigma_s^2}$	$\frac{\sigma}{\sigma_s}$
				0	6	6	6	6	6	$\frac{1}{10}$	0.3162
				1	5	6	6	6	6	$\frac{2}{19}$	0.3244
				2	4	6	6	6	6	$\frac{319}{2852}$	0.3344
			0	2	CONE OFF-LINE	6	6	6	6	$\frac{1}{8}$	0.3536
			1	3		5	6	6	6	$\frac{2}{15}$	0.3651
			2	4		4	6	6	6	$\frac{319}{2214}$	0.3796
		0	2	4		CONE OFF-LINE	6	6	6	$\frac{1}{6}$	0.4083
		1	3	5			5	6	6	$\frac{2}{11}$	0.4264
		2	4	6			4	6	6	$\frac{319}{1576}$	0.4499
	0	2	4	6			CONE OFF-LINE	6	6	$\frac{1}{4}$	0.5000
	1	3	5	7				5	6	$\frac{2}{7}$	0.5345
	2	4	6	8				4	6	$\frac{319}{938}$	0.5832
0	2	4	6	8				CONE OFF-LINE	6	$\frac{1}{2}$	0.7071
1	3	5	7	9					5	$\frac{2}{3}$	0.8165
2	4	6	8	10					4	$\frac{319}{300}$	1.0312

*BASED ON THE FOLLOWING ASSUMPTIONS:

1) OPTIMUM CONE HALF-ANGLE; $\beta = 54.74°$
2) WORST CASE DEGRADATION OF RELATIVE MEAN SYSTEM ERROR; FOR SEQUENTIAL CONE FAILURES

R82-0114-006(W)

APPENDIX F

MAINTENANCE REQUIREMENTS FOR SKEWED SENSORS

1. Objectives

The primary objective of this study is to determine an optimum sensor configuration which will comply with a safety risk goal of 10^{-10} losses per flight hour with a maintenance plan which permits scheduled restoration of redundancy bi-annually (1500 flt hrs.) and no unscheduled maintenance.

The study was accomplished through the evaluation of the following secondary investigation:

- Evaluation of the relative reliability characteristics of Skewed and Orthogonal sensor configurations.
- Determination of the sensitivity of orthogonal and skewed system failure probabilities to variations in configuration complexity, element failure rate and mission time.
- Evaluation of the impact of the bi-annual scheduled maintenance concept.
- Evaluation of the impact of imperfect redundancy management; e.g. less than 100% coverage and a greater than zero false alarm rate.

2. Conclusions

- A skewed sensor set appears to offer the only practical means of achieving the 10^{-10} safety risk probability per flight hour when unscheduled maintenance is eliminated.
- An alternate maintenance concept which permits unscheduled maintenance whenever only 4 skewed sensors remain operational can result in the attainment of the safety risk objective with 20% fewer sensors and a very low probability (.0008)* of performing unscheduled maintenance between scheduled maintenance events. The life cycle cost trade study between the alternate and required maintenance concepts should be performed and used to determine which is the preferred approach.

  * for a sensor failure rate of 20 FPM and 7 skewed sensors (see Paragraph 6.0).

- an analytic approach to false alarms and coverage which was based on a previous study has been extended to the general case of a system of n like items which can be characterized by the binomial expansion. The results of this analysis showed that additional sensor redundancy provides no improvement when the sensor failure rate is 20 failures per million hours. For realistic probabilities of no false alarms (.999) and correct failure isolation (.99), a limit of 10^{-8} failures per hour appears to have been reached. Additional work in applying the concepts of false alarms and coverage to a Markov transition state analysis is recommended. In addition, an approach which takes into account the dependence of the probability of false alarms on mission duration, and allows restoration between missions of sensors which have been removed via false alarms would be more realistic and will be pursued in future studies.

3. Orthogonal vs. Skewed Sensors

A set of n orthogonal sensors would have n/3 sensors aligned along each of the three principal axes of the aircraft. When comparison monitoring is used to detect and isolate failures, a minimum of two sensors per axis is required for safe operation. With two sensors remaining, the next sensor failure would be detected but not isolated, causing operation on incorrect data, which in a Fly-by-wire application, can be considered to result in loss by the aircraft. The reliability of an orthogonal system with n sensors is given by the expression.

$$(1)\quad R_{os} = (R_{axis})^3$$

$$\text{where}\quad R_{axis} = R_s^{\frac{N}{3}} + \frac{N}{3} R_s^{\frac{N}{3}-1}(1 - R_s) + \frac{\frac{N}{3}!}{(\frac{N}{3} - 2)!2!} R_s^{\frac{N}{3}-2}(1 - R_s)^2 +$$

$$+ \ldots \frac{\frac{N}{3}!}{(\frac{N}{3} - m)!m!} R_s^{\frac{N}{3}-m}(1 - R_s)^m .$$

Note that m = total of failures, R_s = sensor reliability, $\frac{N}{3} - m = 2$ and n is an integral multiple of 3

A set of n skewed sensors would have the sensors aligned in predetermined directions none of which necessarily coincide with any of the principal axes or each other. In order to completely define three dimensional space, three independent sensor measurements are required. Whenever 4 sensors remain, safe operation is possible. The next sensor failure would be detected but not isolated by comparison monitoring. Therefore, a skewed set of n sensors can tolerate n-4 failures. The expression for the reliability of a system of n skewed sensors is

$$(2)\quad R_{ss} = R_s^N + N R_s^{N-1}(1 - R_s) + \frac{N!}{(N-2)!2!} R_s^{N-2}(1 - R_s)^2 + \ldots$$

$$+ \frac{N!}{(N-m)!m!} R_s^{N-m}(1 - R_s)^m .$$

Note that n-m=4

The above equations for Ros and Rss apply whenever conditional probabilities do not apply to the scenario under consideration. They are applicable to a sensor system which is maintained in a conventional manner (e.g. unscheduled maintenance as required between misisons), whose false alarm rate is zero, and whose coverage (detection and isolation probability) is 100%.

Using the fact that R sensor $= e^{-\lambda t}$, where λ is the sensor failure rate and t is the mission time, equations (1) and (2) can be used to explore the relative characteristics of skewed and orthogonal sensor configurations.

For a sensor faiure rate of 80 failures per million hours (FPM) and a one hour misison, equations (1) and (2) yield the following equivalence relationships:

6 Skewed => 12 Orthogonal

7 Skewed => 15 Orthogonal

8 Skewed => 18 Orthogonal

This is depicted graphically in Figure 81.

When the number of sensors is fixed at 6 skewed and 12 orthogonal, and the sensor failure rate is held at 80 FPM, equations (1) and (2) are used to show the effect of mission times of 1, 3, 5, and 8 hours. This is depicted in Figure 82. It is noted that mission times of greater than three hours would require additional redundancy in order to attain a 10^{-10} failure per mission goal.

When the number of sensors is fixed at 6 skewed and 12 orthogonal, and the mission time is fixed at 1 hour, equations (1) and (2) are used to show the effect of sensor failure rates of 10, 20, 45, 60, and 80 FPM. This is depicted in Figure 83. It is noted that sensor failure rates as high as 80 FPM would allow attainment of a goal of 10^{-9} failures per hour.

4. Sensor Faiure Rates for the 1990's Time Frame

Before attempting to postulate sensor failure rates based on the technology expected to be available in the 1990's we must first evaluate the actual performance of current technology hardware and assess how well we were able to predict this performance.

The sensor package on the F-14 aircraft is an orthogonal system containing 2 roll rate gyros, 2 pitch rate gyros, and 3 yaw rate gyros. During a recent year of operation, the packages which included these seven rate gyros accrued 52,377 flight hours and experienced 34 in-flight failures. This data yields a failure rate of 649 FPM for the sensor packages and 92.7 FPM for each of the seven sensor elements. This value is reasonably close to the initial prediction of 80 FPM. Also note that the military environment is a more rigorous environment to the gyros than commercial service would be.

The sensor envisioned for a 1990's application would consist of a ring laser gyro, a power switching regulator, and a bus interface unit.

This hardware would provide individual sensor data to a dual 1553 data bus, where remote processors would handle redundancy management and perform flight control, inertial, and other required computations.

The ring laser gyro, which has no moving parts, is currently being incorporated into an IMU for the AV8B. The pREDICTED failure rate for this current technology version of the ring laser gyro is reported to he 20 FPM by the IMU manufacturer. The powre switching regulator which receives aircraft/battery power and transforms it to required gyro power and bias power for electronics, is predicted by MIL HDBK 217 C to have a fialure rate of 10 FPM. The BIU, a current technology version of which is being manufactured at the Grumman Electronics System Center on a single chip, has a current technology prediction of 20 FPM. This would yield a prediction for current technology version of a ring laser gyro and associated electronics of 50 FPM. It is not unreasonable to postulate that based upon the rate of technology improvement, this failure rate will improve to 20 FPM by the 1990's.

5. Scheduled Maintenance

The study requirement for scheduled maintenance bi-annually, with no unscheduled maintenance between missions can be evaluated using equations (1) and (2) when the misison time is set to the flight hours expected to be accrued between the bi-annual maintenance periods (1500 hrs,approx.). In order to determine a risk probability on a per flight hour basis, equations (1) and (2) must be divided by the mission time*.

Figure 84 depicts the number of sensors required for orthogonal and skewed configurations as a function of sensor failure rate. Note thatin this analysis all sensors are powered and operating continuously. Consideration of unpowered "spare" sensors was not undertaken since the finite, non-negligible warm-up time for the laser gyro presents analytical and hardware complications which would tend to offset any advantages.

If the predicted 1990's failure rate of 20 FPM for the sensor element is attained, then 9 skewed and 27 orthogonal sensors are required to attain the safety risk probability goal of 10^{-10} losses per flight hours. If the sensor failure rate were to remain at a current level of 80 FPM then 13 skewed and 42 orthogonal sensors would be required. For all practical purposes, the criteria for no unscheduled maintenance has virtually eliminated an orthogonal configuration from further consideration.

6. Alternate Unscheduled Maintenance Concept

The restriction of no unscheduled maintenance requires the addition of at least 7 skewed sensors (λ = 80 FPM) compared to a scenario that allows unscheduled maintenance between 1 hr. missions. A reasonable alternate to this restrictive scenario would be to permit unscheduled maintenance whenever the system has arrived in a state in which the next failure would result in loss of the aircraft. For skewed sensors, this represents the state in which all but four sensors have failed.

* See Paragraph 8.0 for a discusion of this criterion.

This conditional maintenance criterion introduces a conditional probability of restoration of redundancy into the reliability analysis. This scenario lends itself to treatment via Markov transition state analysis. Using Grumman's existing MARCAP analysis computer program, which facilitates the mechanics of multiplying an initial state vector by transition matrices and restoration matrices to obtain final and intermediate state vectors, the results depicted in Figure 85 were obtained. Note that for a sensor failure rate of 20 FPM, 7 skewed sensors are required to attain a safety risk probability of 10^{-10} losses per flight hour. This represents a savings of 2 sensors over the scenario which allows no unscheduled maintenance.

7. The Impact of False Alarms and Imperfect Coverage on Sensor Reliability

The need to incorporate a criterion for the persistence of failures before permanently disengaging a system element has already been discussed in connection with transient errors in data transmission. This section quantifies the hazards of premature disengagement.

False alarms (removal of n functional units from the system) and imperfect coverage (removing one or more functional units prior to removing the failed unit from the system) reduce system reliability. Consider a three channel, active, parallel redundant system in which two functional units are required for successful operation. With no false alarms and perfect coverage, the reliability would be

$$R = P_0 + P_1$$

where P_0 (probability of successful operation with no failures)

$$= e^{-3\lambda t}$$

P_1 (probability of successful operation with one failure)

$$= 3\left(e^{-2\lambda t} - e^{-3\lambda t}\right).$$

If false alarms are considered,

$$P_0 \rightarrow P_0' = P_0\left[P_{\overline{FA}} + (1 - P_{\overline{FA}})\,(P_{\overline{FA}})\right]$$

$$P_1 \rightarrow P_1' = P_1\left[P_{\overline{FA}}\right]$$

where $P_{\overline{FA}}$ = probability of no false alarms (taken to be independent of the number of units remaining in the system; time-weighted mean value used for this analysis).

If imperfect coverage is also considered

$$P_o' \rightarrow P_o'' = P_o'$$

$$P_1' \rightarrow P_o'' = P_1' \quad [P_I]$$

where P_I = probability that a failure will be correctly isolated to the failed unit.

Thus, with both false alrams and imperfect coverage considered, the reliability would be

$$R = P_o'' = P_1''$$

$$= e^{-3\lambda t} [P_{\overline{FA}} + (1 - P_{\overline{FA}}) P_{\overline{FA}}]$$

$$+ 3 (e^{-2\lambda t} - e^{-3\lambda t}) P_{\overline{FA}} P_I$$

For the general case, with no false alarms and perfect coverage, the reliability may be represented as a binomial expansion.

$$R = \sum_{K=r}^{n} \binom{n}{K} (e^{-\lambda t})^K (1 - e^{-\lambda t})^{n-K}$$

$$= \sum_{K=r}^{n} B(K, n, \lambda, t)$$

where r = number of units required

n = number of units installed

The impact of false alarms and imperfect coverage may be considered in the general case by introducing appropriate coefficients for each term in the binomial expansion. The reliability would be

$$R = \sum_{K=r}^{n} C_{n-k}\, B(K, n, \lambda, t)$$

(3) where
$$C_{n-k} = P_{\overline{FA}} \left\{ \sum_{i=0}^{K-r} (1 - P_{\overline{FA}})^i \right\} \quad K = n$$

$$= P_{\overline{FA}}\, P_I \left\{ 1 + \sum_{i=1}^{K-r} [(1 - P_{\overline{FA}})^i + (1 - P_I)^i] \right\}; \quad r < k < n$$

$$= P_{\overline{FA}}\, P_I \quad K = r$$

In most analog systems, redundancy management is done by comparison monitoring. A monitor threshold is set which controls both parameters, $P_{\overline{FA}}$ and P_I. Broadening the threshold reduces the probability of false alarms while increasing the probability of improper fault isolation. Narrowing the threshold has the opposite effect.

The selection of failure monitor thresholds is investigated in great depth in (ref. 34). This report notes that:

- The distribution of bias error for typical rate sensors subjected to normal quality screening can be characterized by a normal distribution which is essentially truncated at the 3 sigma limits.
- For systems whose accuracy and performance requirements would allow setting the monitor threshold slightly above the $\pm$ 3 sigma limits of the sensor population, false alarm probabilities of .999 are not unreasonable.
- When the monitor threshold is set slightly above the $\pm$ 3 sigma limits, .99 probability of failure detection/isolation (coverage) is not unreasonable. In addition, the lack of coverage occurs when the fialure magnitude is in the +3 sigma to +7.5 sigma and -3 sigma to -7.5 sigma ranges. Failures in these ranges were determined to result in a good sensor being flagged as bad followed by successful detection during subsequent interations of the Failure Detection Routine.

Since time constraints precluded the development of false alarm and coverage transition matrix modifiers, no attempt was made to utilize the Markov process in this investigation. Instead, the binomial technique whcih applies to the situation where no unscheduled maintenance is permitted was modified to account for false alarms and coverage, and the results in terms of additional sensor requirements will be extrapolated to those scenarios described by the Markov process.

To apply equation 3 to the case where 9 skewed sensors are installed and at least 4 are required for safe operation (n = 9, r = 4) we must evaluate C9, C8, C7, C6, C5, and C4. C9 operates on the zero failure term of the binomial, C8 operates on the one failure term; etc. (e.g. K = 9, 8, 7, 6, 5, & 4).

Setting $P_{\overline{FA}}$ = .999 and P_I = .99 in equations 3, we obtain

$$C_9 = 999\ 999\ 999\ 999\ 999\ 999\ 999\ 999$$

$$C_8 = (.999)(.99)\,[1 + (.001) + (.01) + (.001)^2 + (.01)^2 + (.001)^3 + (.01)^3 + (.001)^4 + (.01)^4 + (.001)^5 + (.01)^5 + (.001)^6 + (.01)^6]$$

$$C_8 = .999\ 99$$

$$C_7 = .999\ 99$$

$$C_6 = .999\ 989$$

$$C_5 = .999\ 889\ 1$$

$$C_4 = .989\ 01$$

Applying these coefficients to the respective term of the binomial expansion we obtain the results shown in Figure 86. It is noted that the 9 skewed sensor system which apparently complied with the 10^{-10} failures per hour goal (when the sensor failure rate is 20 FPM) can only achieve a 10^{-8} failures per hour goal when realistic alarm coverage probabilities are introduced.

Figure 87 shows 11 & 13 skewed sensor systems, with P_{FA} and P_I = .999 and .99 respectively. It is noted that these systems with 2 and 4 additional sensors cannot achieve the 10^{-10} failure per hour goal when

the sensor failure rate is 20 FPM. Evidently the false alarms and non-isolatable failures are the prime drivers from a reliability standpoint whenever this failure rate is low. At higher failure rates (λ = 80 or 100 FPM) the added redundancy produces significant improvements as expected.

Figure 88 shows the 9, 11 and 13 skewed sensor systems, with P_{FA} and P_I = .999 and .995 respectively. This improvement in isolation probability was introducted to evaluate its effect upon system failure probability. It is noted that at low sensor faiulre rates the added redundancy again does not provide any benefits. However, the improved isolation probability has brought the 9 sensor configuration closer to the goal of $1x10^{-10}$ failures per hours ($8.3x10^{-10}$). The apparent message is that improvements in P_{FA} and P_I which would make their effects neglible are required, isnce whenever they do have a non-negligible effect, added redundancy does not help.

The above analysis must be considered preliminary in nature. More work in developing the methodology for handling the problems of false alarms and failure to correctly isolate a failed sensor is required. A technique which takes into account the dependence of the probability of false alarms on mission duration, and which permits restoration of a sensor removed via false alarm between missions would be more realistic. This will be our objective for future studies.

8. Failure Per Flight Hour With No Unscheduled Maintenance

The requirements of a 10^{-10} probability of loss per flight hour in a bi-annual scheduled maintenance only scenario (no unscheduled maintenance between missions) has been interpreted in several ways. One interpretation was to design a system with a loss probability of 10^{-10} for the entire 6 mos scheduled maintenance interval. This resulted in a system of 12 skewed sensors (with zero unscheduled maintenance) and 10 skewed sensors with unscheduled maintenance whenever a minimum set of sensors (4) remained. The probability of performing unscheduled maintenance was $.124x10^{-6}$.

The interpretation presented in the earlier sections are systems which provide an average risk per flight hour of 10^{-10}. This required 9 skewed sensors for zero unscheduled maintenance and 7 skewed sensors with unscheduled maintenance whenever 4 sensors remain. For this case the probability of performing unscheduled maintenance has increased to $8x10^{-4}$. (The chances of 3 of 7 failing is higher than the chances of 6 of 10 failing during a given interval.) While this system provides an average hourly risk of 10^{-10} losses per flight hour, the risk in the flights which immediately precede scheduled maintenance is substantially higher than 10^{-10} and the risk in the flights which immediately follow scheduled maintenance is substantially better than 10^{-10} losses per flight hour.

In a conventional unscheduled maintenance scenario, which allows restoration of redundancy as required between missions, the risk is the same for every mission and a requirement for risk per flight hour is meaningful. The elimination of unscheduled maintenance (or the alternate concept of restoring redundancy only when a minimum safe complement of hardware remains) left us with the dilemma of variable risk. In the context of a system in a commercial application, the higher risks incurred prior to scheduled maintenance impose moral, if not legal, implications.

As a compromise between the two interpretations noted above, it was decided to investigate a system which maintains a minimum risk of 10^{-10} losses per flight hour. This can be achieved by restoring redundancy when the number of sensors remaining is equal to that required to yield a minimum risk per hour of 10^{-10}. For the case of a one hour mission and a sensor failure rate of 20 FPM this represents a set of 6 skewed sensors.

A system of 7 skewed sensors with restoration of redundancy when six remain yields an average hourly risk of 10^{-17}, a minimum hourly risk of 10^{-10} and a probability of performing unscheduled maintenance of .195. Except for the considerable chance of performing unscheduled maintenance the system meets all of our objectives. Adding additional sensors will reduce the average hourly risk while reducing the probability of performing unscheduled maintenance. Figure 89 shows the probability of performing unscheduled maintenance as a function of the number of sensors installed. Note that in order to reduce the probability of unscheduled maintenance to a chance of one in ten thousand, ten sensors must be installed. For a ten sensor configuration with redundancy restored when six remain our minimum hourly risk is 10^{-10} while the average hourly risk is 10^{-20}. This system at the expense of 3 additional sensors over the configuration described earlier, has desirable safety characteristics, with a correspondingly low chance of unscheduled maintenance.

Figure 90 is a representation of the relative hourly risk characteristics for the various interpretations of the system reliability goals.

From the above it is apparent that the maintenance scenario is a major driver of system configuration. The ultimate interpretation of the requirements with respect to maintenance and hourly risk probability should be decided and mutually agreed to.

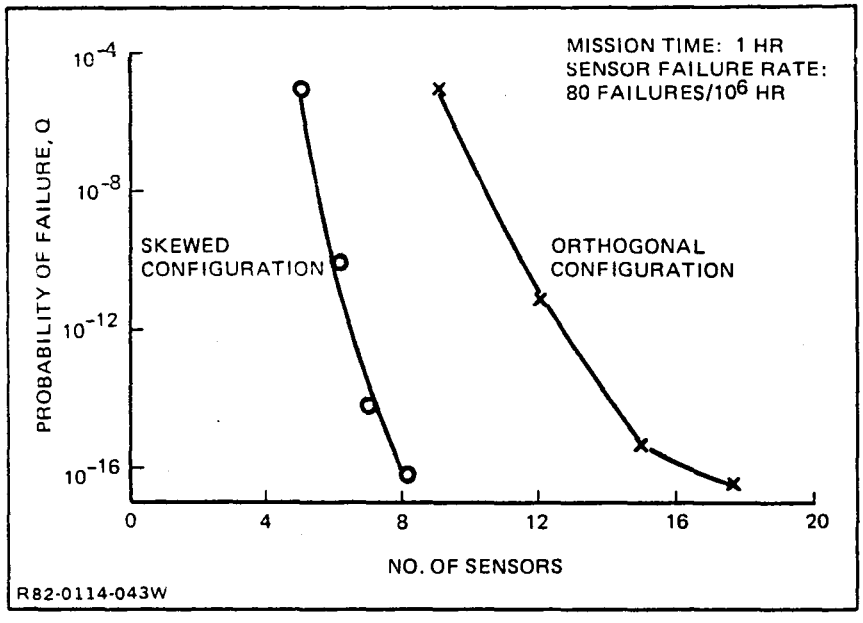


Figure 81 Sensor Configuration, Skewed vs. Orthogonal

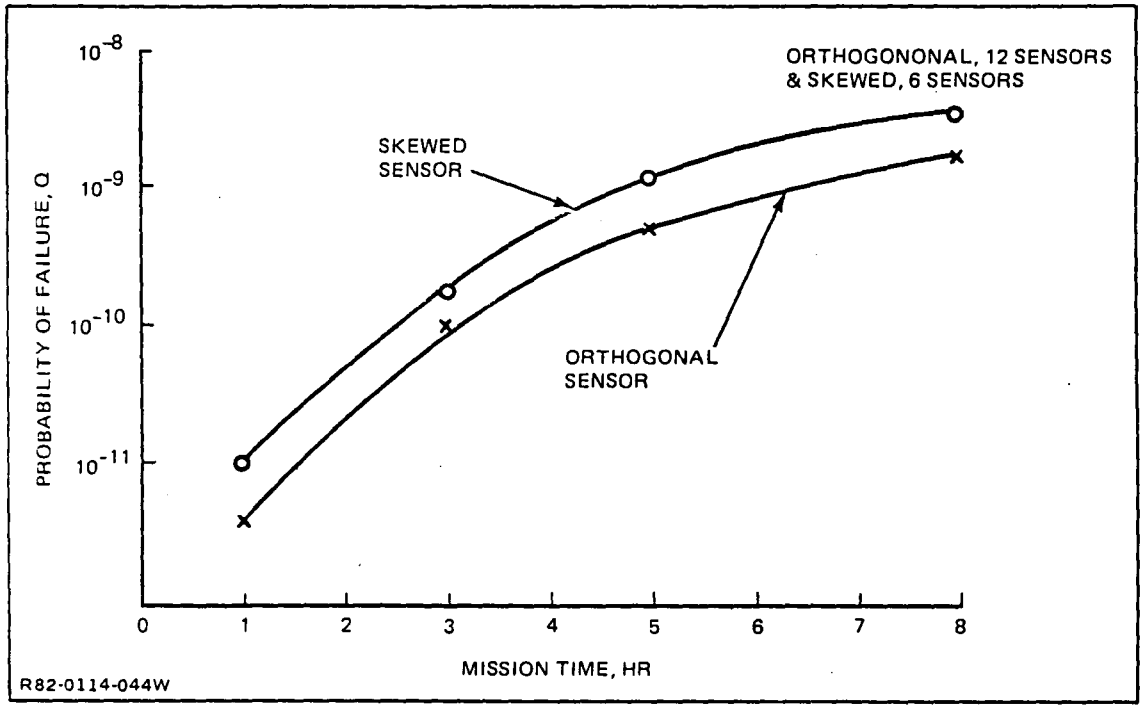


Figure 82 Unreliability vs. Mission Time

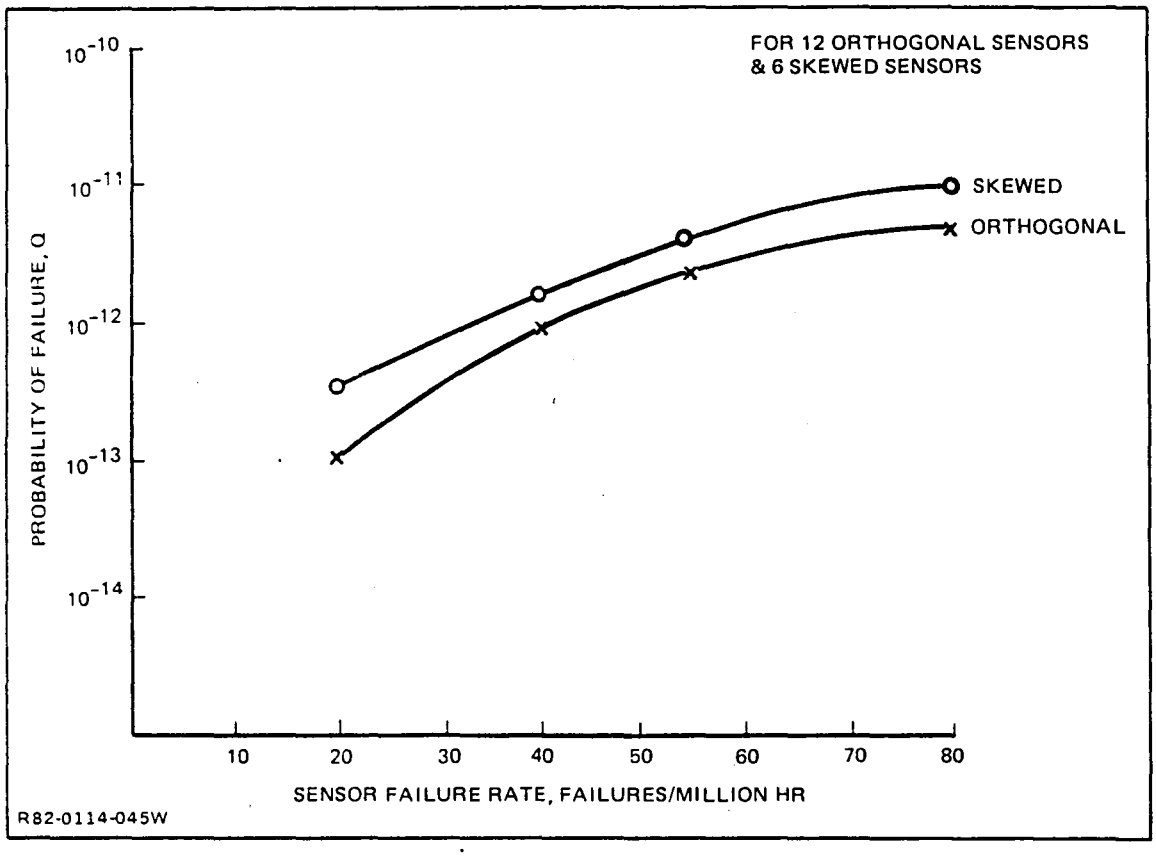


Figure 83 Effect of Sensor Failure Rate

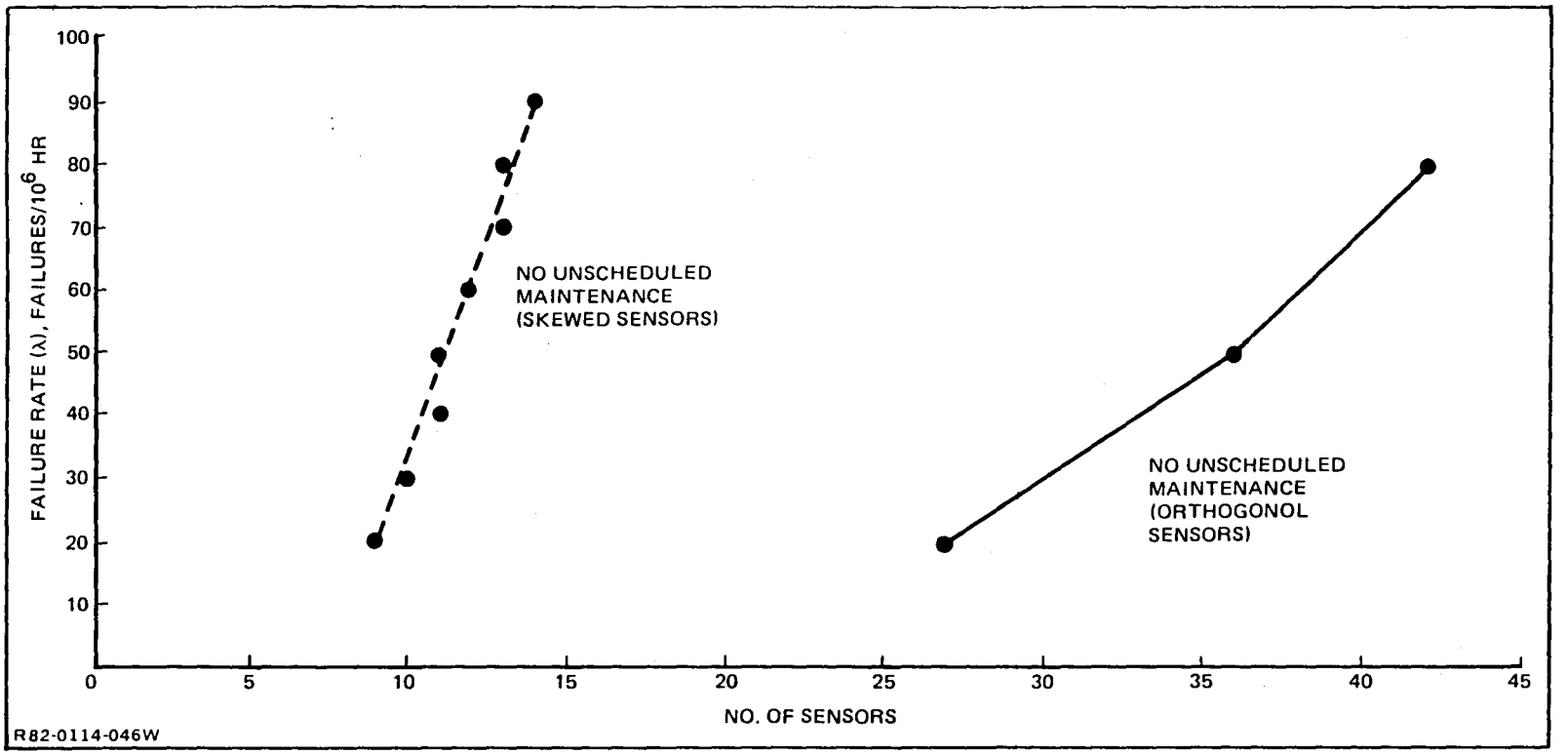


Figure 84 Sensors Required for Probability of Failure $\leqslant 10^{-10}$ Failures/Hr

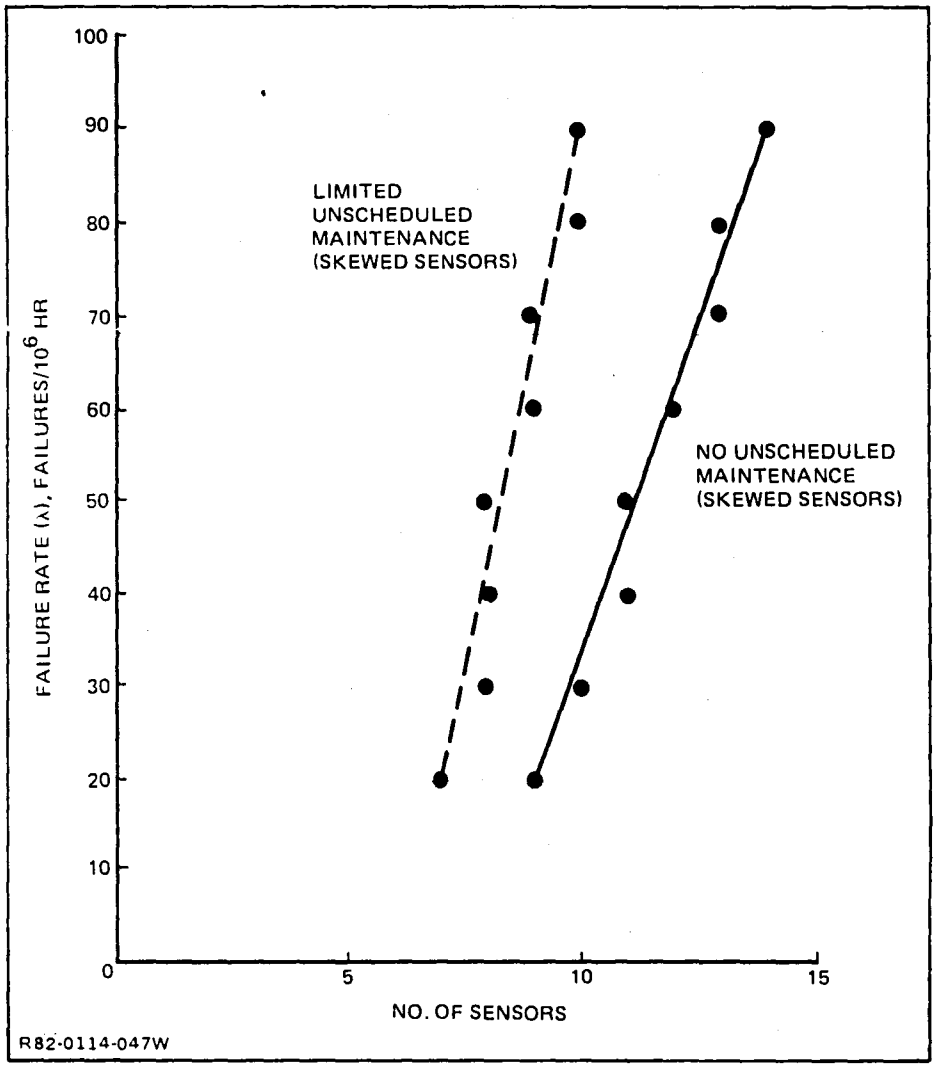


Figure 85 Sensors Required for Probability of Failure, $\leq 10^{-10}$ Fail/Hr

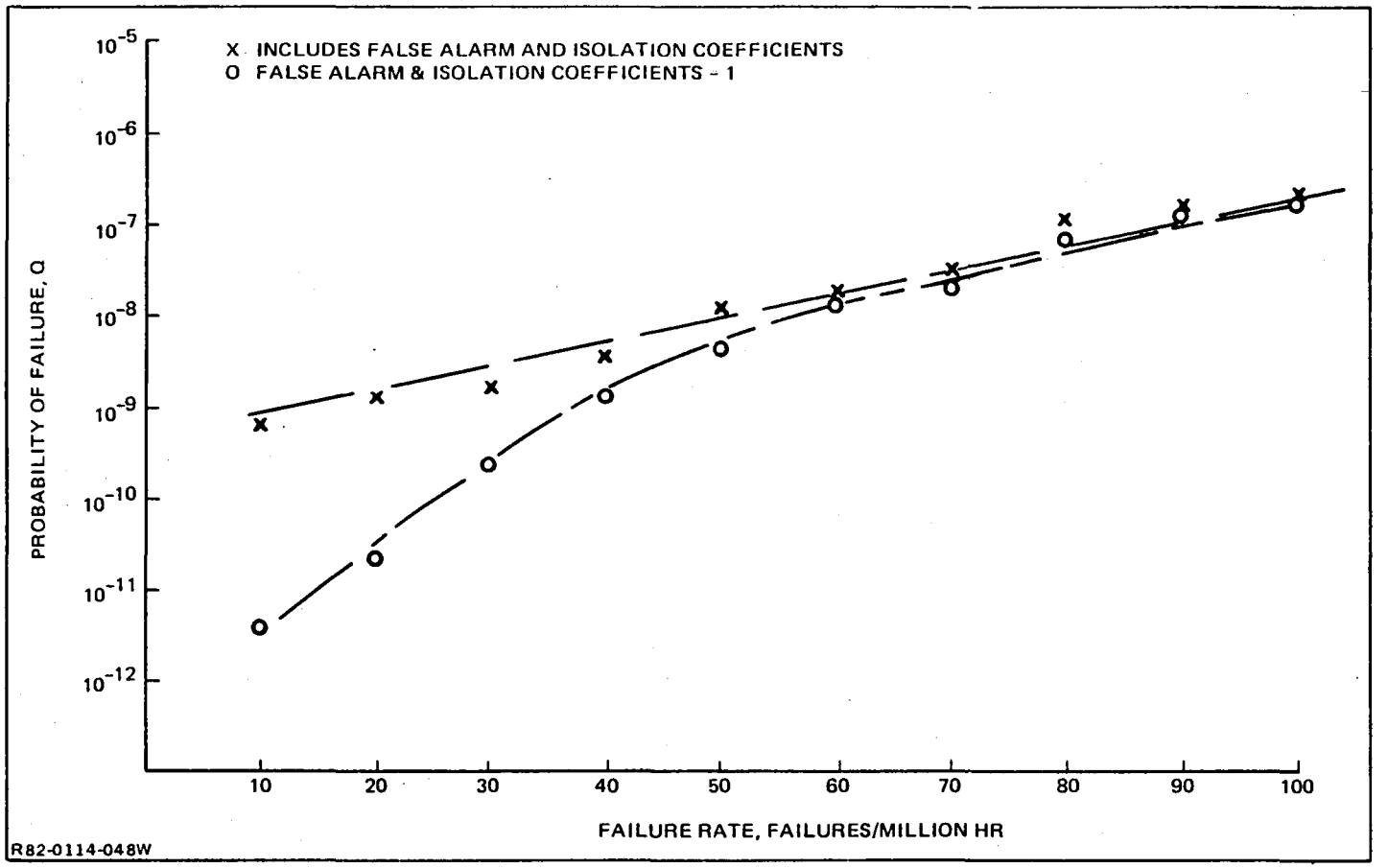


Figure 86 System Unreliability, 9 Skewed Sensors With & Without False Alarm & Isolation Coefficients

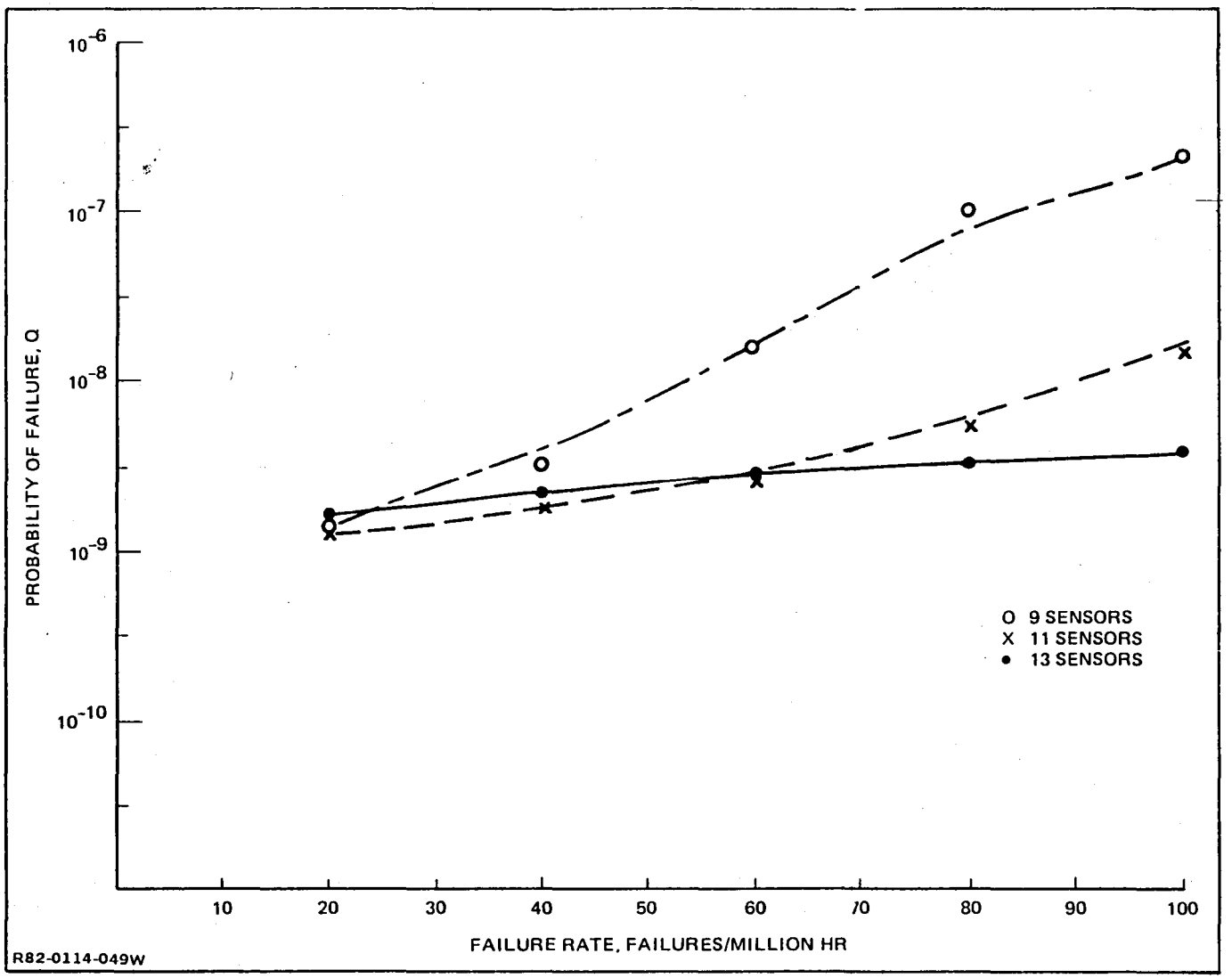


Figure 87 Effect of Added Redundance with $P_{\overline{FA}} = 0.999$ & $P_I = 0.99$

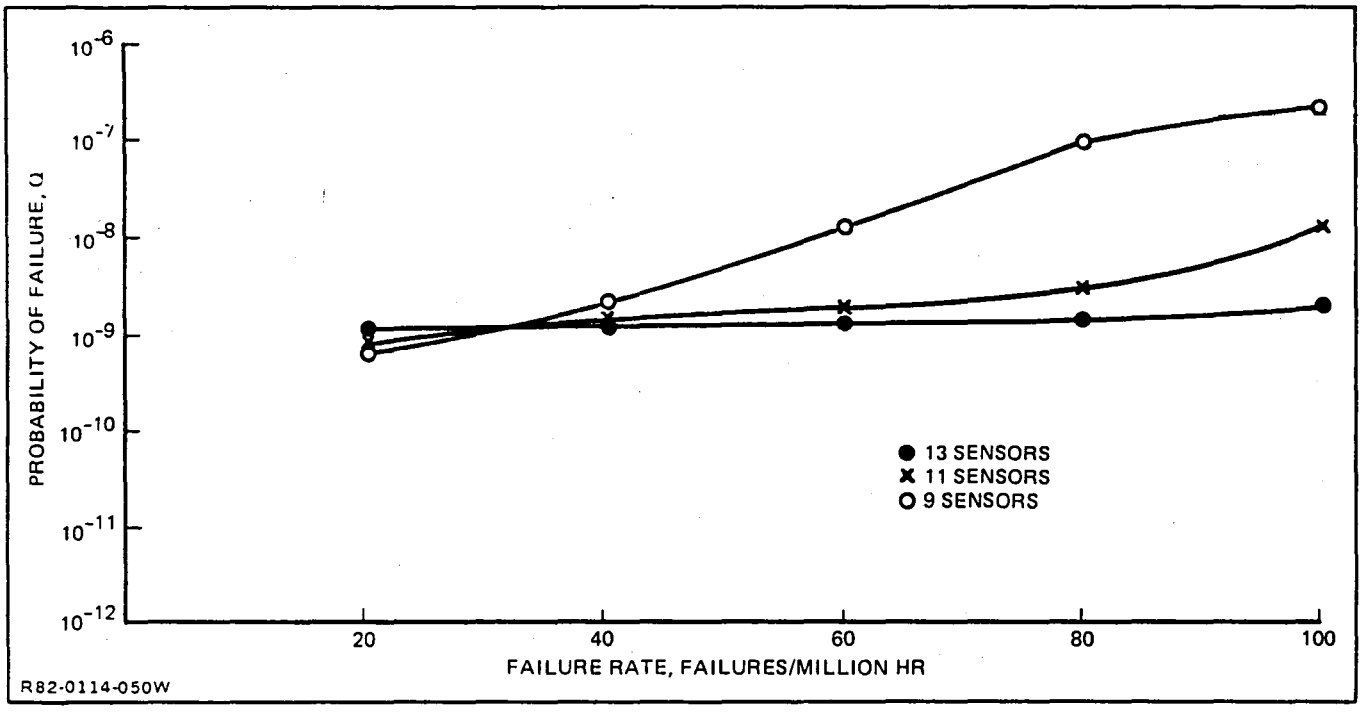


Figure 88 **Effect of Added Redundancy with $P_{\overline{FA}} = 0.999$ & $P_I = 0.995$**

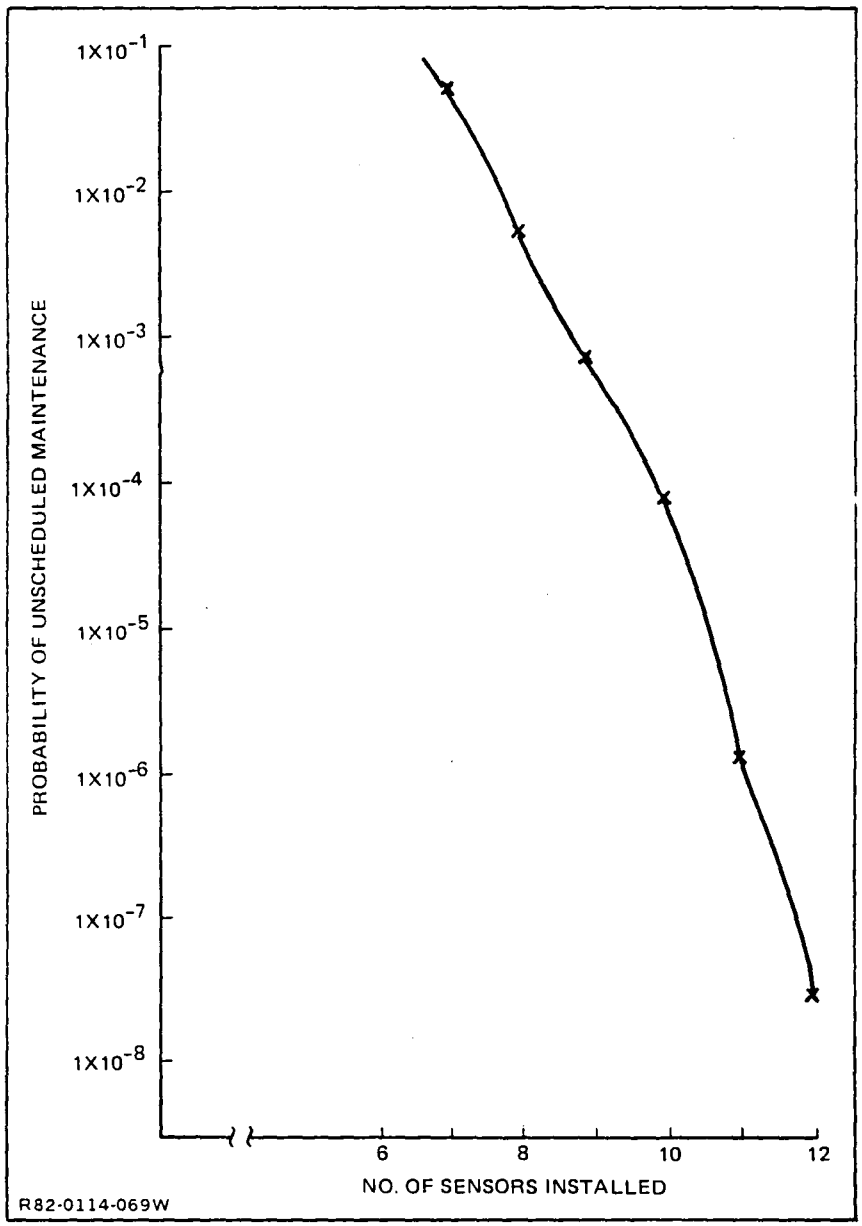


Figure 89 Probability of Unscheduled Maintenance vs No. of Sensors Installed (Unscheduled Restoration when Six Sensors only Remain, Sensor Failure Rate 20 fpm)

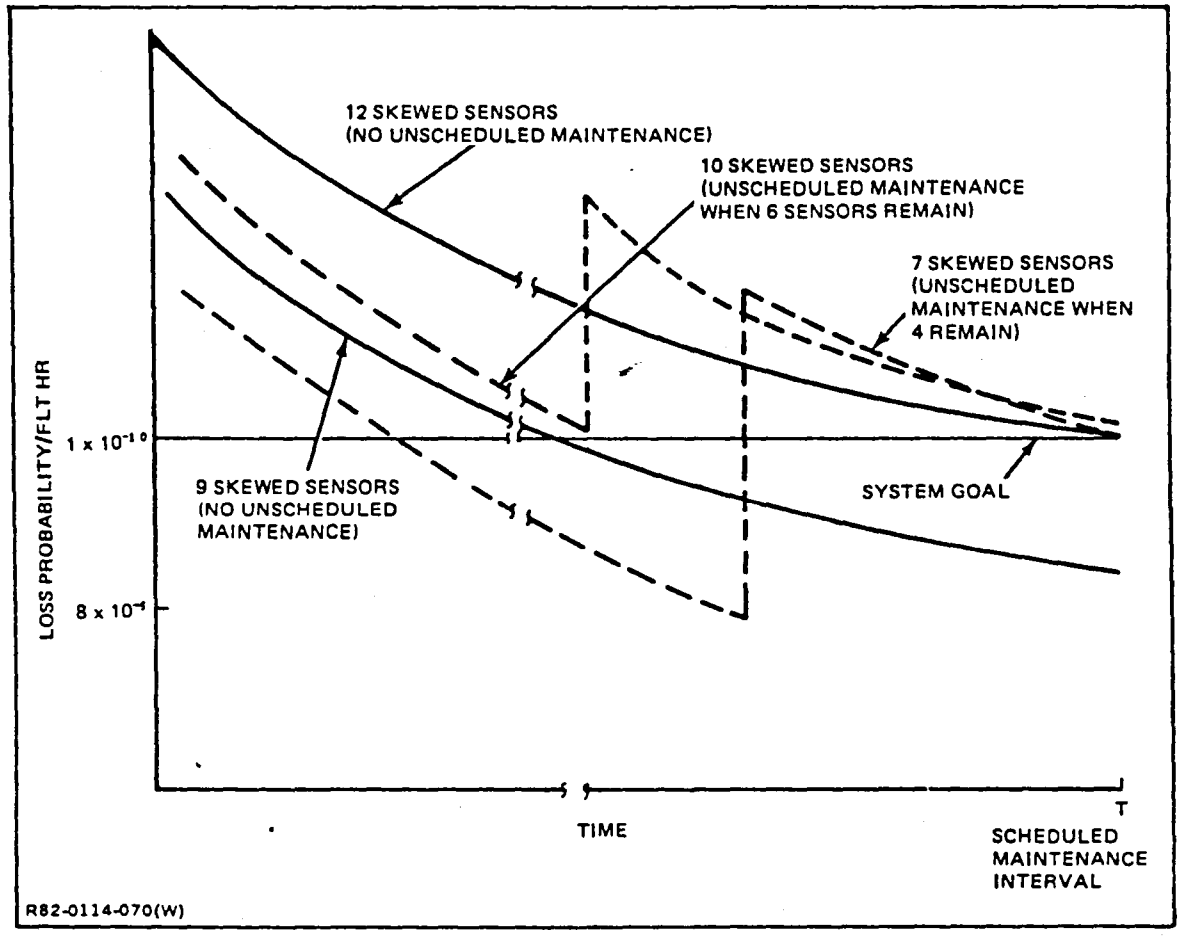


Figure 90 Schematic Representation of Loss Probability per Flight Hour for Interpretations of Safety & Maintenance Requirement

APPENDIX G

SYSTEM INTEGRITY BETWEEN MAINTENANCE ACTIONS

1. Introduction

In paragraph 6.1.3.3 of the S.O.W., it was required to allow for periodic maintenance with a "high degree of integrity" between maintenance actions. As it transpired, "high degree of integrity" was subject to several interpretations, each of which lead to a different set of maintenance requirements. For this reason, and because the meaning of total system survivability was also affected by these interpretations, it was decided to dedicate a separate appendix to the subject.

2. The Meaning of 10^{-10}/hour Survivability

Throughout the study, the threshold survivability requirement of each candidate subsystem was assumed to be 10^{-10}/hour. When these subsystems were combined, it was expected that the survivability of the flight control system would be of the order of 10^{-9}/hour. These loss rates are subject to two possible interpretations.

Interpretation #1

In this interpretation "10^{-10}/hour" is viewed as an average rate of loss of function of the subsystem. It is obtained by dividing the total member of failed subsystems by the total number of operating hours. Accordingly, it is not required that the probability of subsystem failure during each and every flight hour be less than 10^{-10}. It is only the average that counts. This was the interpretation adopted for the study.

Interpretation #2

In this interpretation "10^{-10}/hour" is viewed as the maximum failure rate allowed during each and every flight hour.

Example:

The life of a subsystem is arbitrarily subdivided into operational periods of T hours, each. It is known that the probability of subsystem failure during each period is P. The following parameters are easily computed:

1. Average number of periods to loss of subsystem = 1/P

and

2. Average time to loss of subsystem = T/P (hours).

Thus,

3. Average number of losses per hour = P/T.

When computing the spares required:

T = maintenance period and

P = function of the number of spares required.

According to Interpretation #1, the number of spares was determined to satisfy the inequality.

4. $P/T \leq 10^{-10}$/hour.

Because of the successive losses of spares, it is clear that survivability, by any interpretation, is a decreasing function of time during any maintenance period. As a consequence, when spares are determined by (4), the probability of loss of subsystem during the first hour of flight is several orders of magnitude less than 10^{-10}, whereas during the last hour of flight, it is several orders of magnitude greater than 10^{-10}. The average, however, over the entire maintenance period is always 10^{-10}/hour or less.

According to Interpretation #2, on the other hand, an additional number of spares would have to be carried to insure that the probability of loss of subsystem never exceeded 10^{-10} for any flight.

A very conservative criterion of insuring this requirement is to compute the number of spares using the inequality.

5. $P \leq 10^{-10}$

This could lead to a prohibitively large number of spares. Moreover, when

T = 1500 hours

the resultant average loss rate is

$$\frac{10^{-10}}{1500} = 0.66 \times 10^{-13}/\text{hour}$$

which clearly far better than what is required as an average.

3. Conclusions

(1) Throughout the study and, in particular, when computing spares, the survivability goal of 10^{-10}/hour was interpreted as an average rate of loss and, accordingly, does not require that the probability of loss of subsystem during each and every flight hour never exceed 10^{-10}. This interpretation appears to be consistent with the method which established the survivability goal in the first place, i.e., by dividing the number of aircraft losses by the total number of operating hours of all aircraft in service.

(2) The use of inequality (5) resulted in an average survivability of 0.66×10^{-13}/hour. This appears to be exceedingly small. In addition, this interpretation results in a larger number of spares.

(3) Interpretation #2 could have been employed as described in Appendix F, Section 8 at a cost of a few additional spares. The resultant average loss rate would undoubtedly be significantly less than 10^{-10}/hour and the probability of performing unscheduled maintenance could become significant.

(4) The crux of the problem of interpretation is that for conventional unscheduled maintenance between missions the average and maximum risk are equal. For a scenario of scheduled maintenance only, the average risk and maximum risk can differ by orders of magnitude. It is this disparity which can raise moral or even legal implications for a commerical transport application.

APPENDIX H

DESCRIPTION OF GULFSTREAM II STA MODIFICATION

1. STA Description

The Shuttle Training Aircraft (STA) is a modified Grumman Gulfstream II which is configured for training Orbiter pilots from 35,000 feet to the actual Orbiter cockpit height above the runway at Orbiter touchdown. The Orbiter descent trajectory as well as responses to Orbiter pilot control commands are accurately duplicated by the STA. High-fidelty Orbiter cockpit-motion matching is accomplished by the model following system implemented in the Simulation System computer.

The STA provides Orbiter pilots with a realistic reproduction of Orbiter cockpit motions, visual cues and handling qualities while simultaneously matching the Orbiter's atmospheric descent trajectory from 35,000 ft altitude to touchdown. This is accomplished with independent control of six degrees-of-freedom, effected with the standard autopilot control on pitch, roll and yaw and with the use of auxiliary direct lift and side force control surfaces (DLC and SFC) and in-flight reverse thrust. These controls are illustrated in the aircraft three-view presented in Figure 91. The motion of the auxiliary surfaces as well as the conventional aircraft controls are commanded by the DAS (Digital Avionics System)

The STA can perform nine training cycles in a 3 1/2-hour flight from altitudes in excess of 35,000 ft while maintaining an 8,000 ft cabin altitude. Its operating envelope everywhere equals or exceeds Orbiter training requirements. The 1400 cu ft cabin and 5600 lb payload potential provides a large capacity for future utility growth.

The STA has sufficient structural strength to accommodate all critical STA design load conditions. All modifications have been designed for minimum structural scarring and maximum use of existing components, support brackets, etc. All STA actuators are either existing Gulfstream II equipment or off-the-shelf hardware in present use on other Grumman aircraft. Primary control system actuators are of dual tandem type driven by two completely independent hydraulic systems, either of which can supply the required power.

The DLC (direct lift control) is designed to match the Orbiter visibility angle and normal acceleration changes with angle-of-attack throughout the entire STA operating envelope. The DLC provides this capability for all Orbiter and STA gross weights both in and out of ground effect. A safe margin above the training mode stall speeds is always maintained. The DLC is flutter-free and the Gulfstream II wing box and flap support fittings are retained.

The DLC surfaces are 22.5% chord plain fast-acting flaps. These flaps occupy the same wing span as the basic Gulfstream II Fowler flaps and utilize the same flap hard points. The outboard half of the DLC also provides roll control in conjunction with the existing ailerons and replaces the lateral control function provided by spoilers on the production Gulfstream II. The DLC can also be operated as a conventional landing flap and ground spoiler.

The outboard segment of the DLC (flaperon) replaces the Gulfstream II spoilers while providing the same roll control power. The spoilers were discarded from the STA as they would produce unsatisfactory flying qualities at certain flight conditions.

The SFC's (Side Force Control) produces 0.1g of side acceleration at Orbiter landing speeds and at maximum aircraft gross weight. They simulate Orbiter sideslip angles and associated changes in side acceleration to side-slip angles beyond $\pm 10^{0}$ at the final approach condition. The SFC design minimizes significant reductions in side force effectiveness with increasing wing angle of attack and landing gear deployment. The SFC's do not measurably alter the lateral/directional stability characteristics of the Gulfstream II. Their deflection does, however, produce a small wing-induced rolling moment which is easily cancelled through the model following computer.

The SFC's are a pair of rectangular surfaces mounted in parallel underneath the wing-fuselage near the aircraft center of gravity. The SFC's are fitted with geared lead tabs and individual end plates to maximize their effectiveness. They are hydraulically-driven, fully-powered surfaces. The SFC's rotate about a torque tube which is itself rigidly fixed (non-rotating) to the wing.

The SFC's are self-contained assemblies with integral actuators, hydraulic, and electrical systems. They are designed for ease of maintenance and removal, ready access, and have a permanently-sealed attachment to the wet aircraft wing.

The Simulation System drives the STA control systems in accordance with the model-following technique to simulate Orbiter cockpit motion and visual cues. The brain of the Simulation System is the Sperry Digital Avionics System (DAS). The DAS is integrated with prototype Orbiter and standard off-the-shelf navigation, control, and cockpit equipment. The capability of the onboard avionics to simultaneously match STA and Orbiter short period motions and trajectory has been demonstrated in all critical areas. The DAS computer software includes all the functions necessary for a complete STA mission.

With the exception of the SFC's and removal of the main landing gear doors for the simulation mission, the outboard appearance of the STA is otherwise unchanged from the production Gulfstream II. Except for the spoilers, the control systems, linkages, and actuators have not been modified for the STA mission. Structural and control system modificatoins are kept to an absolute minimum.

The training pilot occupies the left side of the STA cockpit which incorporates all salient Orbiter instruments and controls, including a Rotational Hand Controller (RHC) and the Multifunction Cathode-Ray Display system (MCDC). An instructor pilot occupies the right-hand seat which is arranged as a standard Gulfstream II. This pilot can assume command of the aircraft at any time and can disengage the STA simulation computer at the push of a button.

The interior of the STA cabin is fitted with the furnishings commensurate with its training mission. Seats are supplied for the instructor pilot, Orbiter pilot, simulation engineer, and one passenger.

The Mach/Airspeed limitations for simulation, simulation fidelity and basic STA are shown in Figure 92.

The STA simulation mode load factor envelope is shown in Figure 93. The simulation mode design structural envelope is from 0.0g to 2.0g with a cut-out to 0.5g above 280 KEAS. The STA requirement for simulation fidelity within the structural envelope, is from 0.8g to 1.5g.

The load factor envelope for the STA out-of-SIM (flaps, symmetrical flaperons and SFC's zeroes and gear up above 250 knots) is the same as the Gulfstream II, -1.0g to 2.5g.

2. Crew System & Equipment

The Gulfstream STA flight compartment and cabin are ideally suited for the Advanced Flight Control System mission. The aircraft is fully conditioned with pressurized air to provide a 7,000 ft. cabin altitude at the maximum FAA certified aircraft altitude of 43,000 ft., with a maximum cabin ΔP of 9.45 PSI. The controlled crew environment has been further enhanced by employing the most modern state-of-the-art thermal and acoustic treatments to the aircraft interior.

The large cabin volume of 1,400 cu. ft. and its payload of 5,600 lbs. provide for an efficient equipment layout with sufficient space for future add-on experiments and installations. The entire STA electronics package, along with the other major avionics equipment, is located within the cabin area, providing easy crew access during flight.

3. Flight Compartment Instruments and System Controls

The flight compartment, located forward of bulkhead FS133, provides side-by-side accommodations for both pilots. The current STA cockpit is configured to functionally represent the flight station of the orbiter. The LH flight station duplicates the orbiter's instrumentation, controls and external visibility angles, while the RH flight station is configured as a standard Gulfstream GII cockpit. Instruments and controls are arranged to permit full operation of the aircraft from the RH seat.

Instruments and systems controls are located in five main groups as shown in Figures 94 and 95. These are:

- Flight/engine instrument panels
- Overhead/eyebrow panels
- Center control pedestal/quadrant
- Center radio control console
- Side consoles

In the STA, the LH side arm control column and control wheel have been replaced with a NASA furnished orbiter side-arm controller. The Gulfstream rudder/foot pedal controls were replaced with an F-14 type mechanism. The increased height of the instrument panel (to accommodate the CRT units) necessitated the removal of the structure at the lower part of the

instrument panel. In addition, the nose wheel steering control was relocated from the LH side console to the RH side console. The instrument panel glare shield was completely revamped to accommodate all the orbiter functions/controls. The current STA cockpit arrangement is shown in Figure 95.

4. Flight Station Rework for Advanced Flight Control System

The general arrangement for the modified Gulfstream is shown in Figure 96. The STA cockpit can be reworked to a Gulfstream type flight station with the advanced instrumentation and controls. The STA instrumentation and controls and a portion of the RH flight station can be deleted and replaced with the defined instrumentation. The instrument panels are to be removed and discarded. Items noted in Tables 16 and 17 are to be removed from the LH console, center console and control pedestal/quadrant.

In order to accommodate the double row of CRT displays at the RH station, the same type of work is required as was performed on the LH side to accommodate the orbiter flight controls. That is, the Gulfstream rudder/brake controls and supporting structure have to be removed and replaced with an F-14 type of mechanism. Both stations will now have the new rudder/brake mechanisms. The same support structure for the lower part of the RH station instrument panel needs to be installed as is on the LH station. Wiring, cables etc. behind the instrument panel have to be relocated to a distance of 15" to provide clearance for the CRT's being installed. Additional secondary support structure will have to be added to support the total of six (6) new CRT's at both flight stations.

New instrument panels and glare shields with instrumentation as shown on Figure 97 can be installed. The left and right consoles and center radio console can be revised to accommodate controls as shown. The forward throw of the control column has to be reduced approximately 5^{o} - 10^{o} to eliminate contact with the new instrument panel location.

Figure 98 shows the arrangement of the flight/engine instrument panel at both stations. Each flight station has two CRT's to show all parameters for flight control. In each case the CRT's have backup flight instrumentation grouped around them. The center panel contains two side-by-side CRT's to show warning annunciators and diagnostics. The co-pilot's panel contains the standard engine tape indications, landing gear control and windshield wiper controls. Additional panel area is available on the left and right and center panels for add-on instrumentation, if required. All radio/communication and FBW controls are located on the center pedestal within easy reach of both pilots. The L/R consoles contain control elements similiar to those on the Gulfstream II. The one exception is the nose wheel steering control wheel on the RH console. The control pedestal is common to the Gulfstream quadrant.

5. Visibility

Visibility is identical to that of the standard Gulfstream II. The maximum practical vision is provided for both pilots, thru six windows. A two-panel windshield is installed forward of the pilot's station, permitting unobstructed vision of 18^{o} down and 16^{o} up, and unobstructed aximuth angles of 25^{o} right and 15^{o} left. The windshield is free to expand and contract without distorting structure. Electrical anti-icing is provided. Two electrically heated direct vision windows are installed adjacent to the main windshield panels. These panels can be opened and permit unobstructed vertical vision of more than 20 up and down.

Two non-opening windows are installed aft of the direct vision windows. These are electrically defogged and permit unobstructed vision angles of 12^{o} up and 25^{o} down. Maximum aft vision is better than 115^{o} along the horizon.

6. Crew Seats

The pilot and co-pilot's seats, mounted on tracks, are capable of forward, aft and vertical adjustment. The vertical adjustment range achieves a reference eye position for pilots with seat to eye heights ranging from 28 to 33 inches.

7. Electronics and Vestibule Area

The area between FS133 and FS206 contains the main entrance doorway and stairs, vestibule, storage compartment, jump seat, and electronic equipment compartment. Currently, the standard electronic boxes and STA related components are located in the RH equipment compartment. Removal of noted STA items (Figure 99) provides sufficient room to install an additional radio altimeter receiver transmitter. The remaining electronic items; navigation, communication, inertial navigation, distance measuring equipment, automatic direction finder, flight director and magnetic tape recorder remain in their present locations. A slide out, adjustable, jump seat is provided in the forward part of the electronic compartment. A control station is provided to the right of the jump seat station for use by the observer seated at this station. Controls include a weather radar scope, RMI, ICS, oxygen control, remote compass compensator (2), compass controller, flight recorder and encoder, and master caution panel. Figure 100 shows the FBW electronic rack installation.

The header installation between FS133 to FS181 provides an oxygen mask, lighting control panel, circuit breaker panel, and seat restraint system for the observer in the jump seat. A life raft, forward inverter box, flash tube power supply and growth volume is provided on the left side of the compartment between FS181 and FS207.

8. Jump Seat

One adjustable and stowable jump seat is installed on the right hand side, just behind the cockpit bulkhead STA 133 in the lower portion of the radio rack. The jump seat is flush with the inboard edge of the radio rack when in the stowed position and is covered with a hinged door.

9. Flight Compartment Finishing

The materials used for finishing the flight compartment are the same type and quality as used elsewhere in the aircraft. The reduction of pilot fatigue, the minimization of compartment reflections and maintaining a high level of safety, has always been a continuing effort at Grumman.

10. Lighting

- Flight Compartment Lighting

  All lights and related equipment are accessible for ease of maintenance. All instruments are integrally lit with white natural lights, edge light panels use white lighting. Instrument panel flood lighting is white. A white map light is provided at each pilot station and jump seat, each being mounted on a flexible shaft

  properly located for optimum utilization. A spare lamp container is provided on the LH console.

- Interior Cabin Lighting

  - Overhead Lighting

    Six (6) overhead dome lights are installed throughout the cabin providing the main cabin lighting.

11. Main Cabin

The area between FS206 and the pressure dome contains the passenger compartment (FS 206-497), lavatory compartment (FS 497-539), and baggage compartment (FS 539 - pressure dome). The STA cabin interior contains an aft facing seat and flight test equipment pallet on the LH side and an avionic "J" box and STA digital avionic system pallet. The first three articles will remain while the STA pallet is removed. In its place, five (5) pallets and one (1) work station are added. This arrangement is shown on Figure 96.

12. FBW Pallets (See Figures 101, 102, 103)

Five (5) pallet modules are provided for installation in the cabin area. All five pallet structures are the same in size and configuration. Each pallet attaches to the seat tracks with four (4) quick disconnect fittings. Each pallet is configured to contain four (4) electronic units, namely; sensor interface unit, actuator interface unit, bus controller, and an application processor. The top portion of the pallet contains a test panel and a status panel. Three (3) sensor component assembly units are mounted to the vertical surface of the pallet. The units are located 120 with respect to each other. Three (3) pallet assemblies are located on the RH side of the cabin and two (2) on the LH side. The pallet design is readily modified to hold up to nine electronic units of 1/2 ATR size.

13. FBW Monitor/Work Station Pallet (See Figure 104)

A FBW monitor/work station can be located aft of the rear facing seat on the LH side of the fuselage. This work station is configured to be operated by a seated occupant. Four (4) fittings on the pallet secure the unit to the seat tracks. The work station contains a writing surface, fault panel, monitor panel with three CRT's and data recording controls. The operator will have sufficient controls and displays on this console to monitor the FBW system and operate the data system.

14. FBW Pallet Installation

Figure 105 and 106 depict a cross section of the cab in showing the relative location of the pallets to each other. A 23 inch angle is provided between the units.

15. Furnishings

- Cabin Seating

  One single rear facing seat is provided for the engineer. It includes base tracking for proper adjustment up to the console, recline and swivel for easy egress. Provisions for life vest stowage is located under the seat. The seat is attached to the floor tracks with quick disconnect type fittings. A side console is located outboard of this seat providing an ICS volume control, head set jack and small item stowage.

- Survival Equipment

  An FAA approved life vest is provided for each crew member. Stowage area is placarded and convenient to the user. An FAA approved life raft with full survival kit and emergency locator transmitter is provided. Stowage area is placarded (left hand forward electronic compartment), installation is such permitting quick and easy access.

16. Lavatory

A lavatory compartment is provided between FS 497 and FS 539. It contains a chemical toilet, hand rail, storage cabinet, paper dispenser and a trash container. A stowage compartment/shelf, with adequate tie-down provisions is provided on the LH side of this compartment. Sliding full length drapes across the bulkhead opening provides privacy in this compartment. A speaker is located in the aft bulkhead.

17. Fire Extinguishers

a portable chemical fire extinguisher is mounted on the Fwd side of FS 133, RH side, behind the co-pilots seat. An H_2O fire extinguisher is mounted to the Fwd, LH side, of the lavatory compartment bulkhead.

18. Oxygen Masks/Bottles

The flight crew has the Gulfstream type fixed oxygen installation. The test engineer, in the cabin is provided with a portable oxygen bottle with mask. This unit is located outboard of his seat. Another portable oxygen bottle, with mask, is located in the lavatory.

19. Baggage Compartment

The baggage compartment is located between FS 539 and the pressure dome. A netting with tie down provisions is used to contain the baggage in this compartment.

20. Interior Finish

The main cabin is fully insulated and lined with 1/2" thick scott felt. Aluminum straps are employed to retain the scott felt in place.

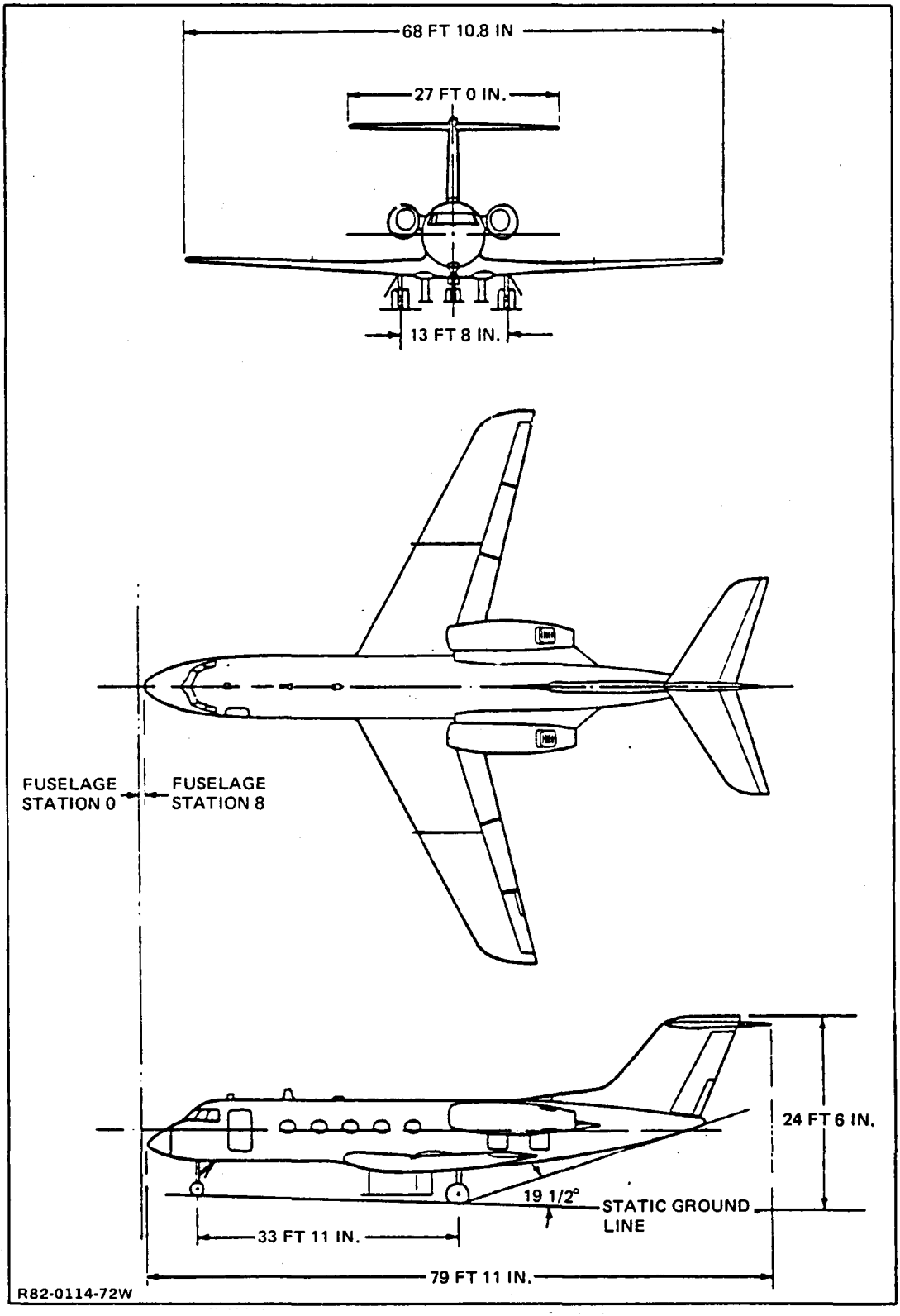


Figure 91 **Shuttle Training Aircraft General Dimensions**

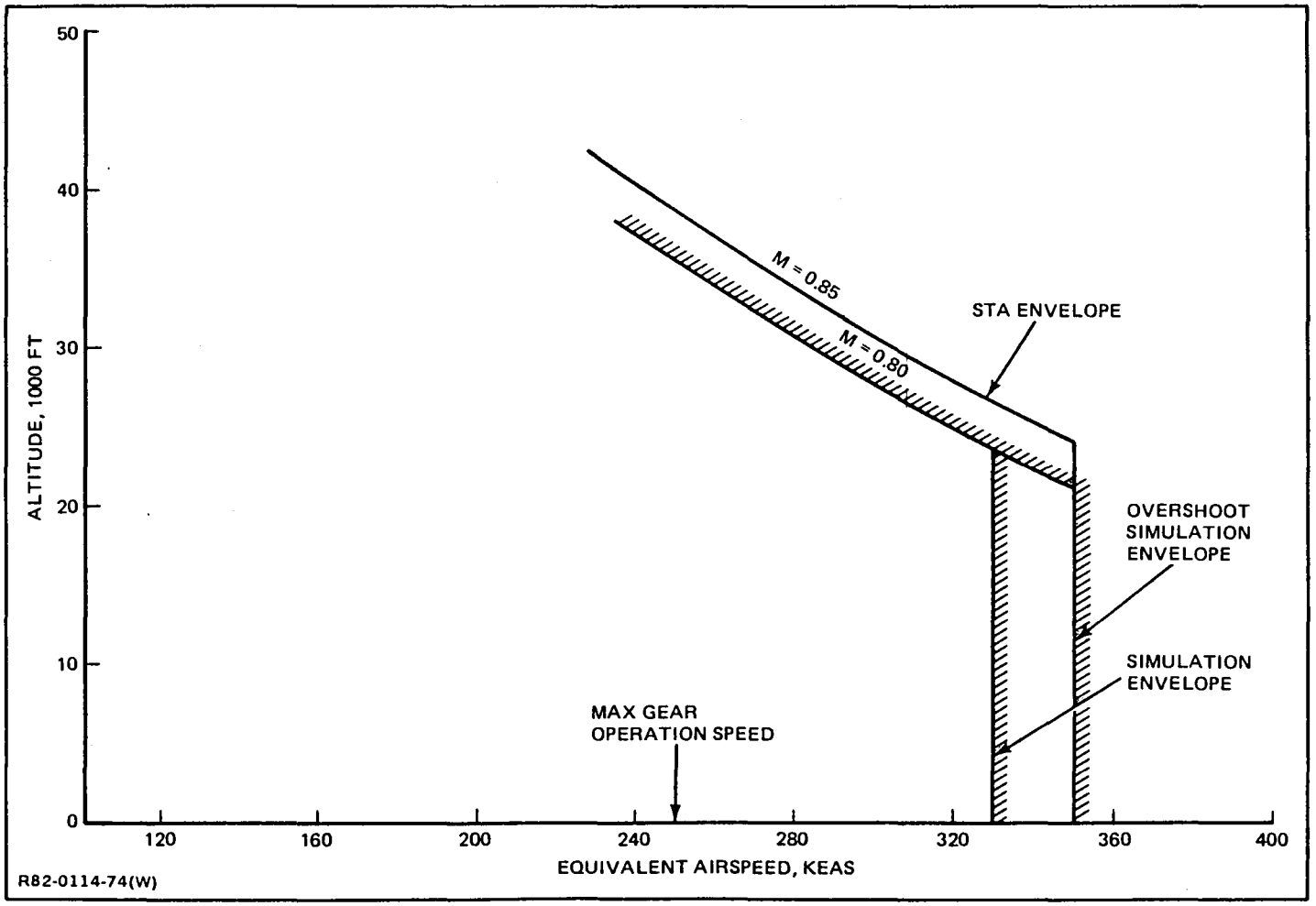


Figure 92 STA Airspeed Altitude Envelopes

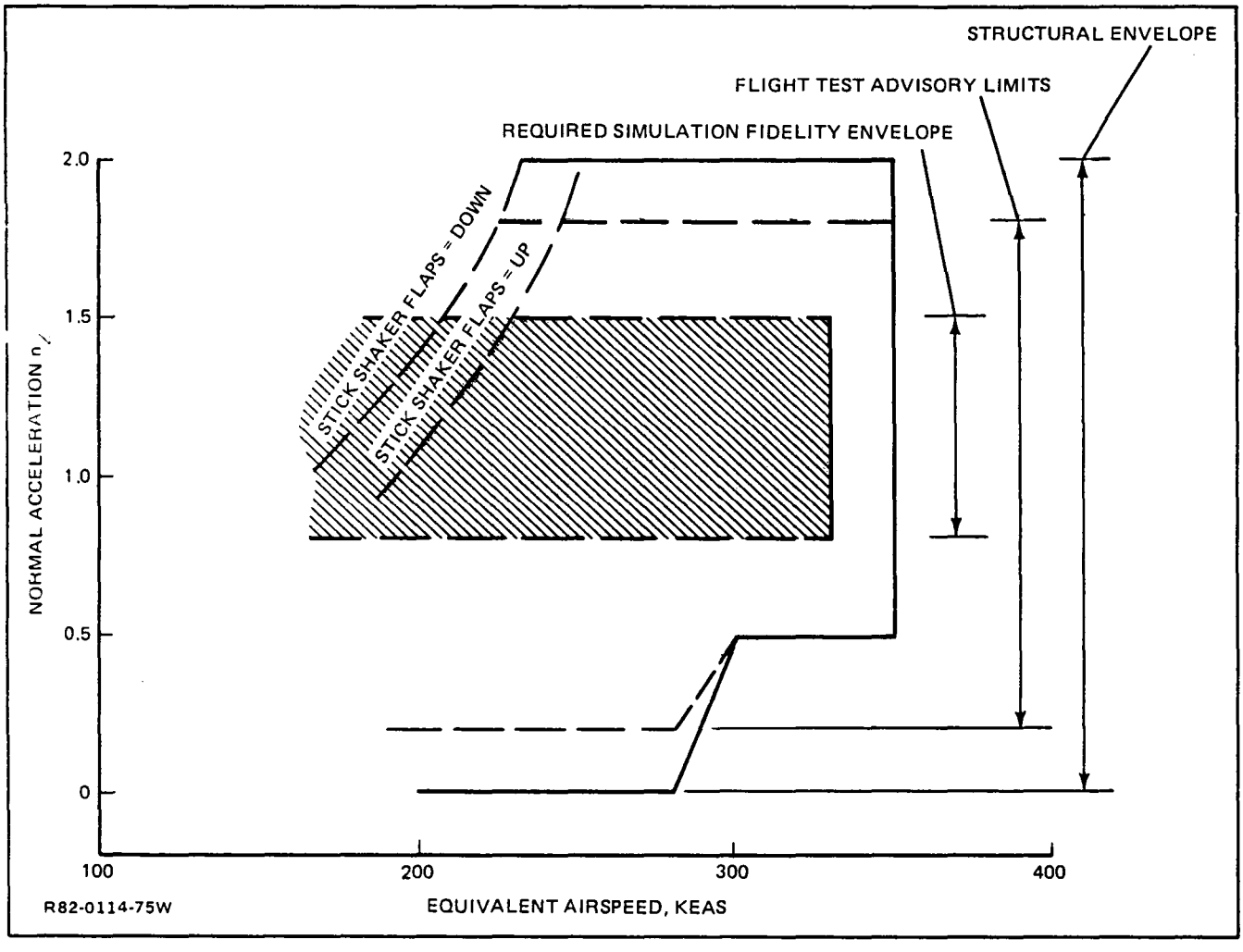


Figure 93 STA Load Factor Envelope

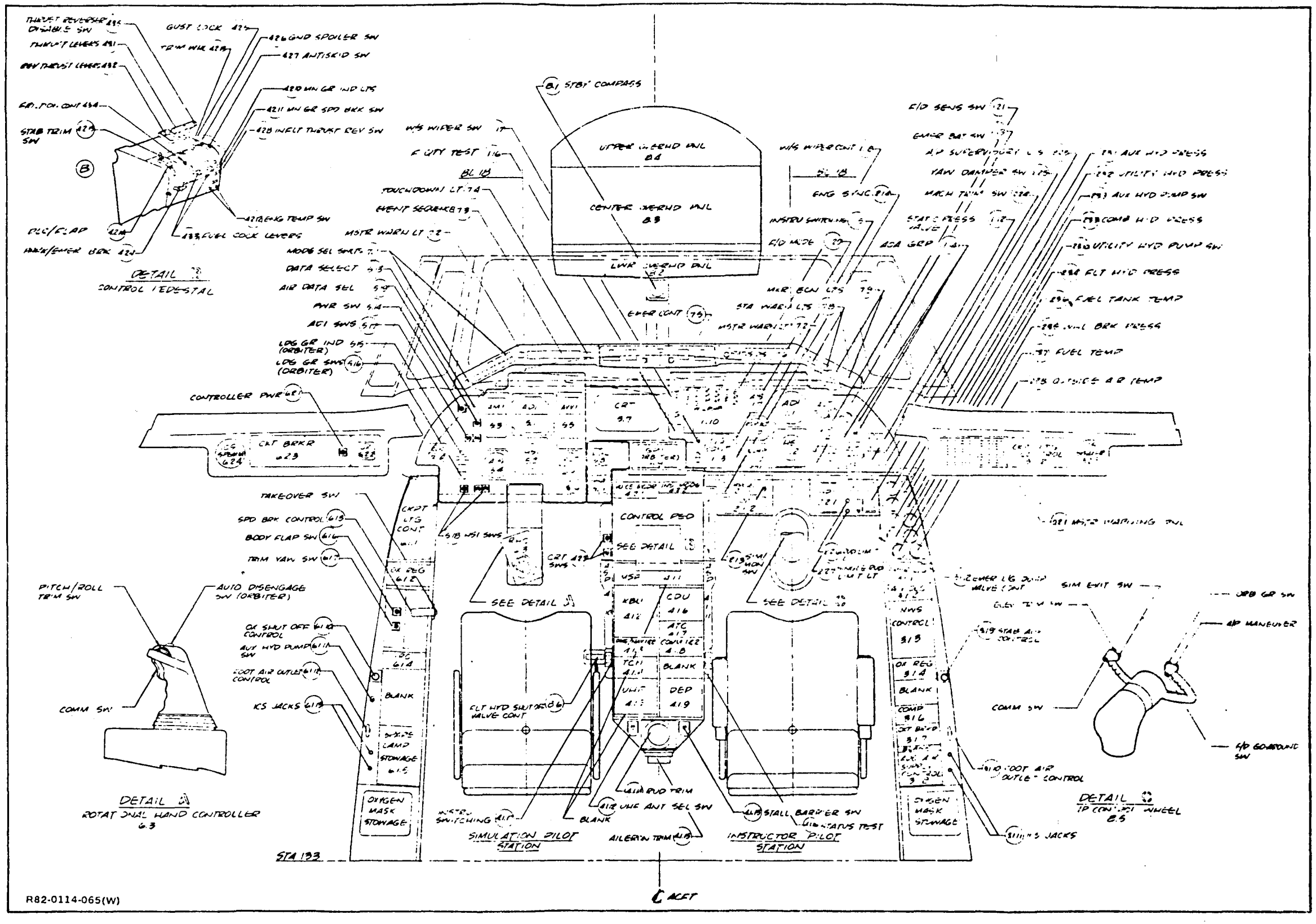


Figure 94 STA Cockpit Arrangement

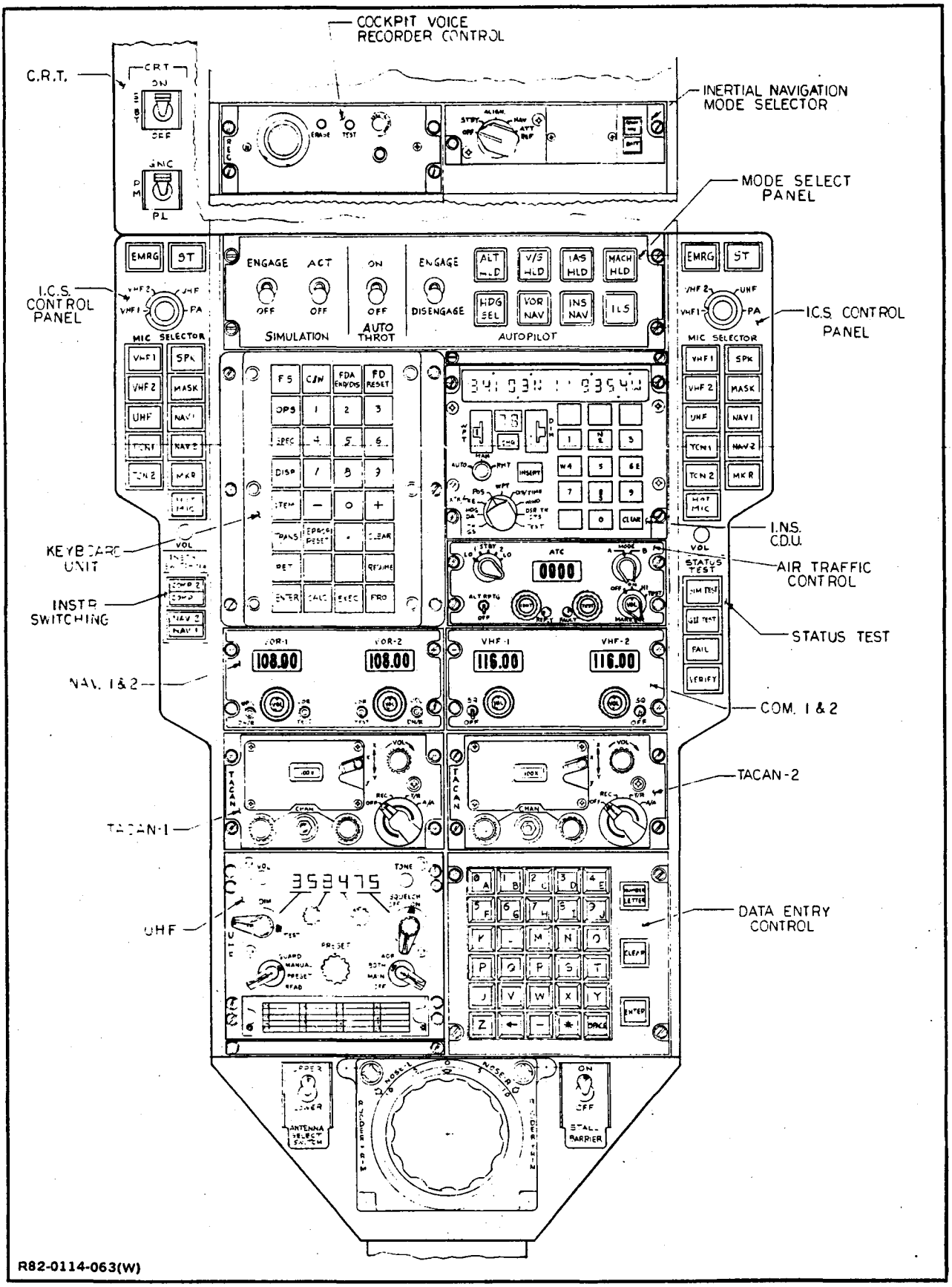


Figure 95 STA Radio Pedestal Arrangement

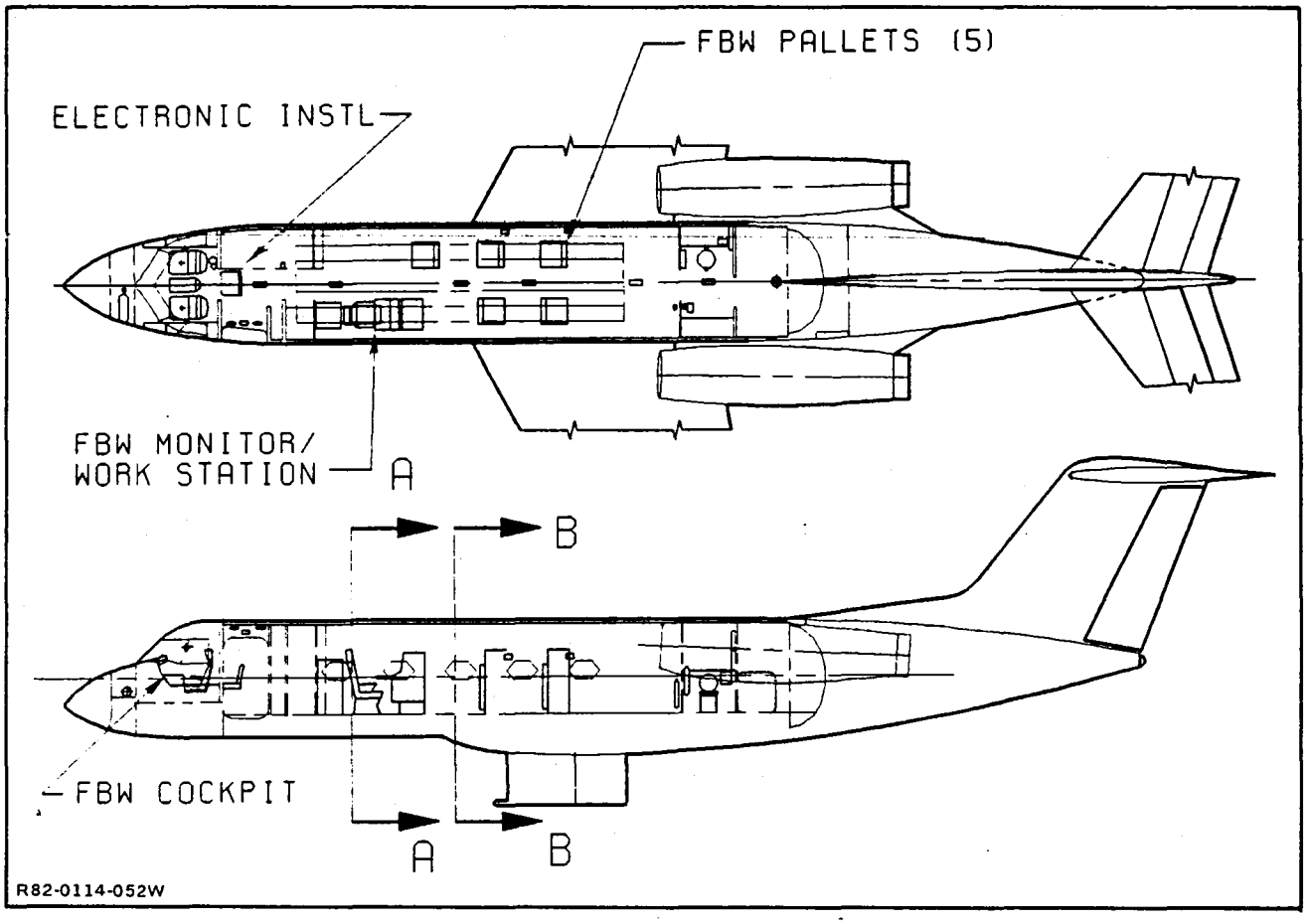


Figure 96 FWB Gulfstream Arrangement

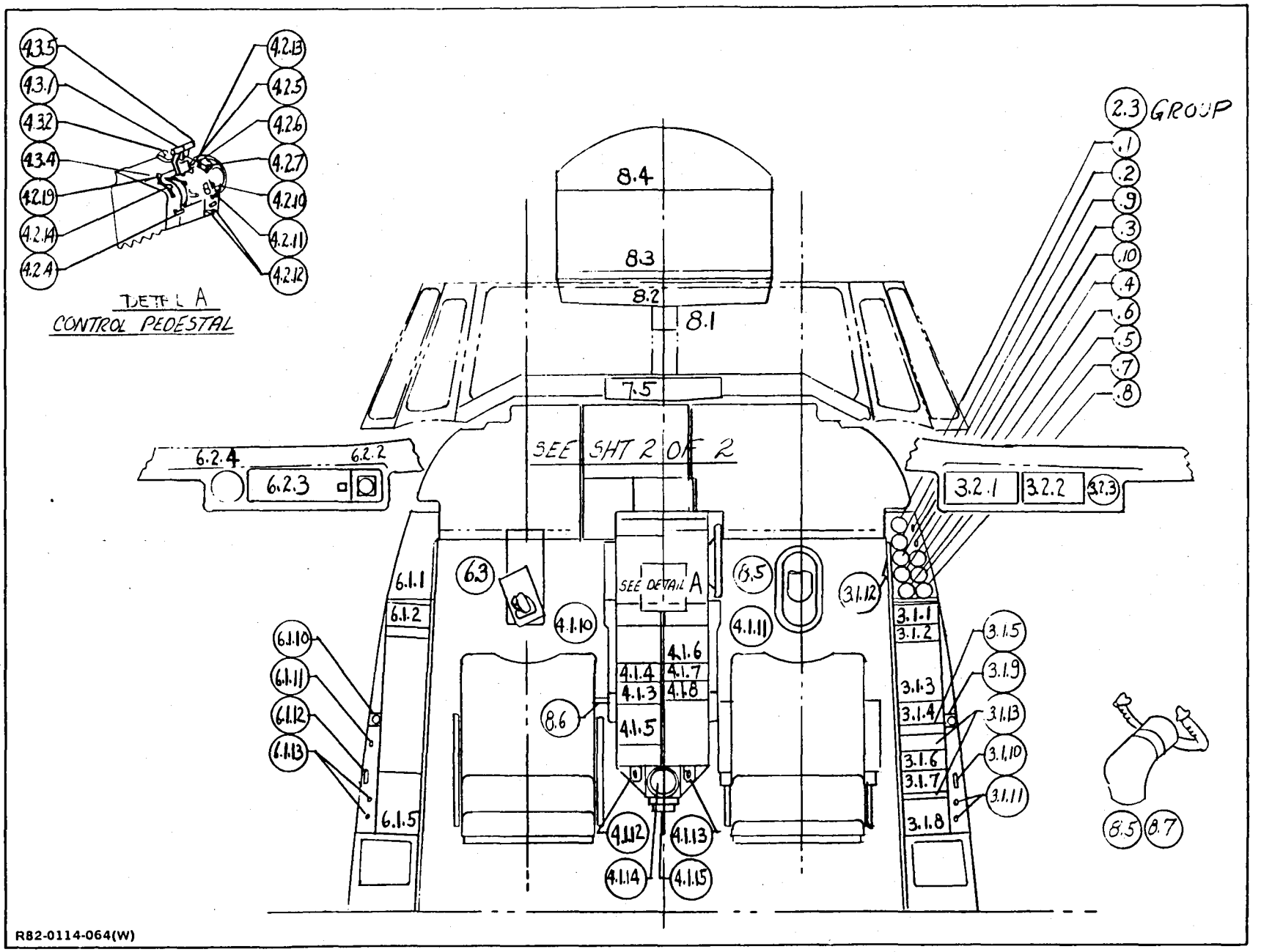


Figure 97 FBW Gulfstream Cockpit Arrangement (Sheet 1 of 2)

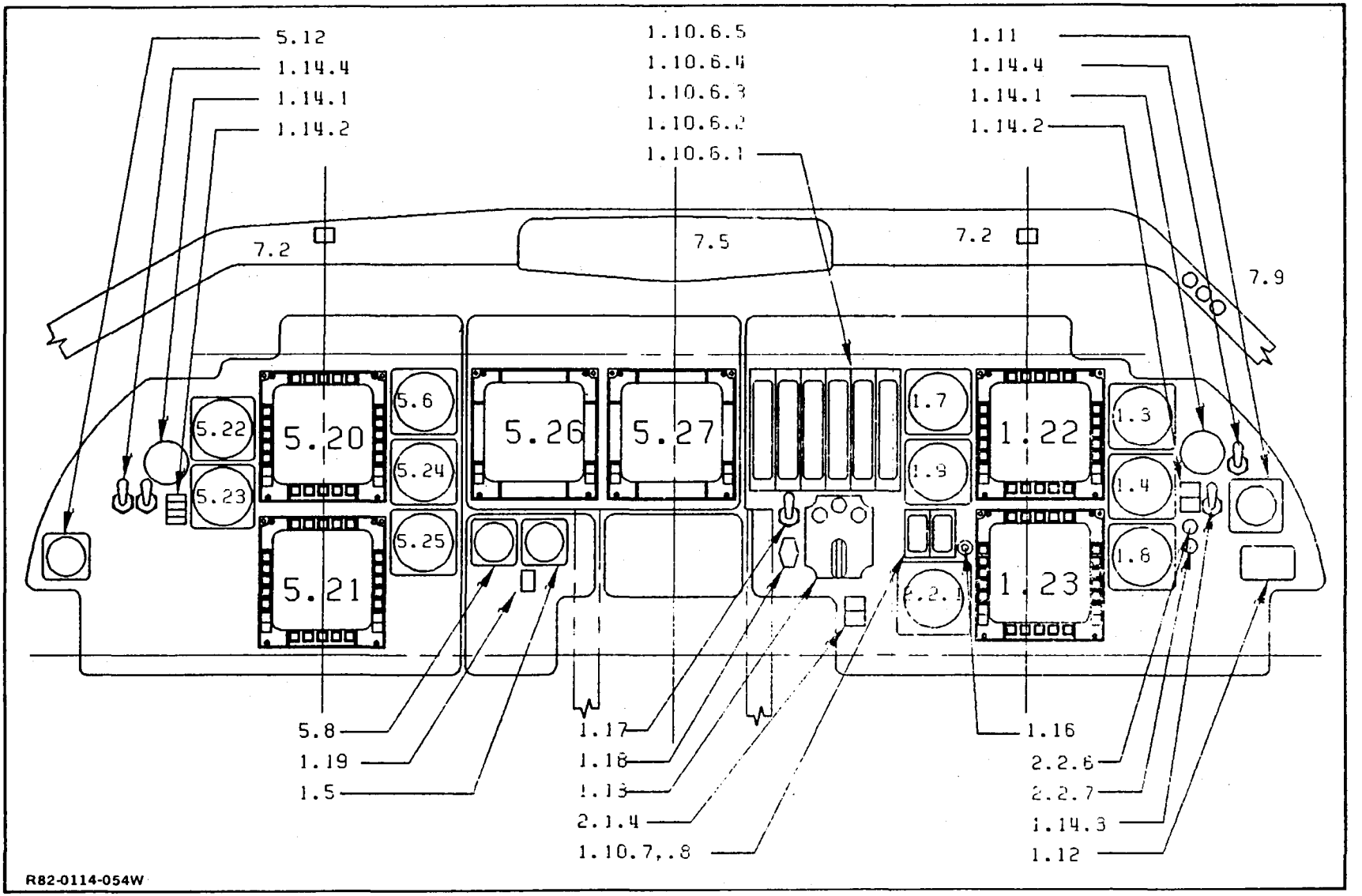


Figure 98 FBW Gulfstream Cockpit Arrangement (Sheet 2 of 2)

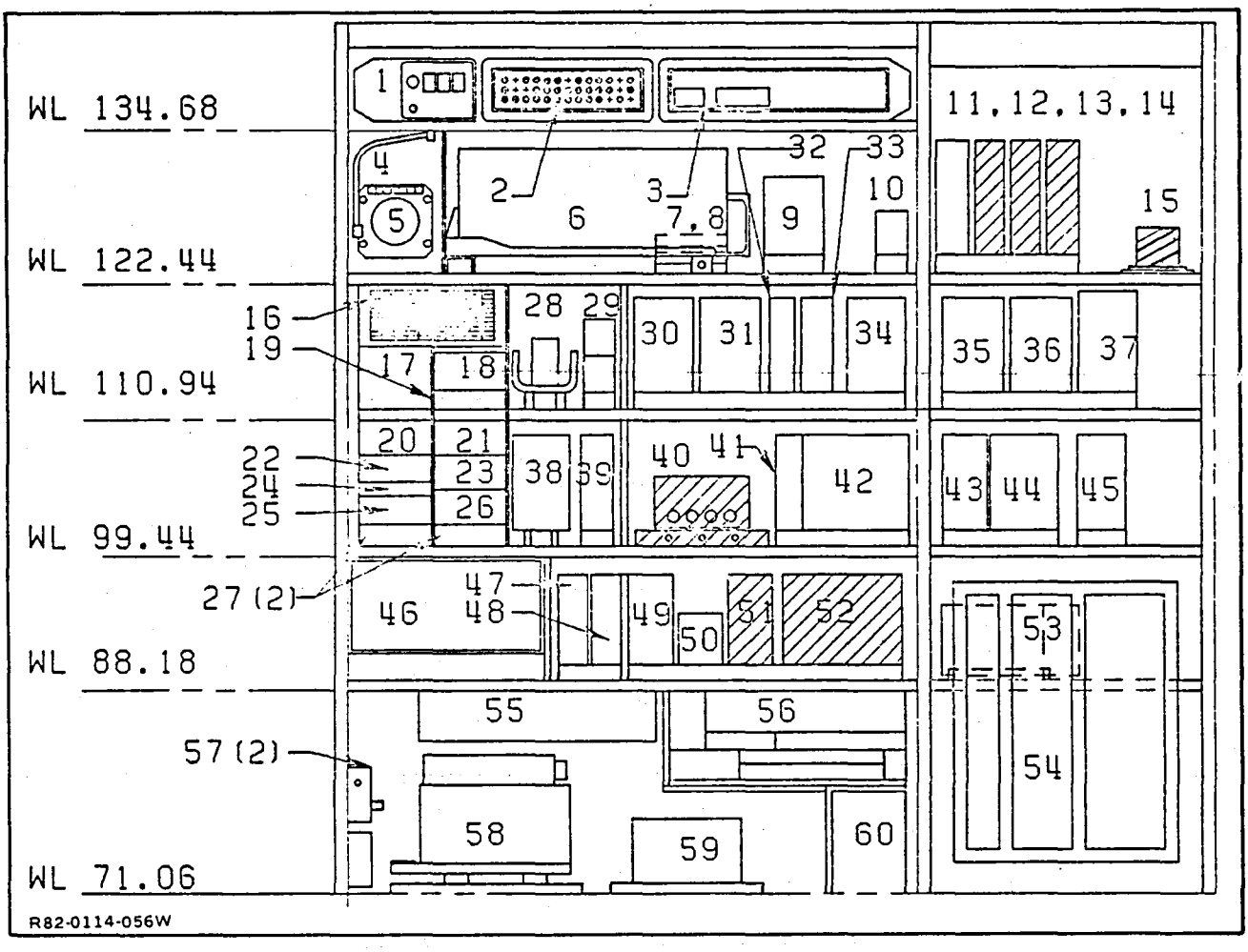


Figure 99 STA Electronic Installation, R/H Side

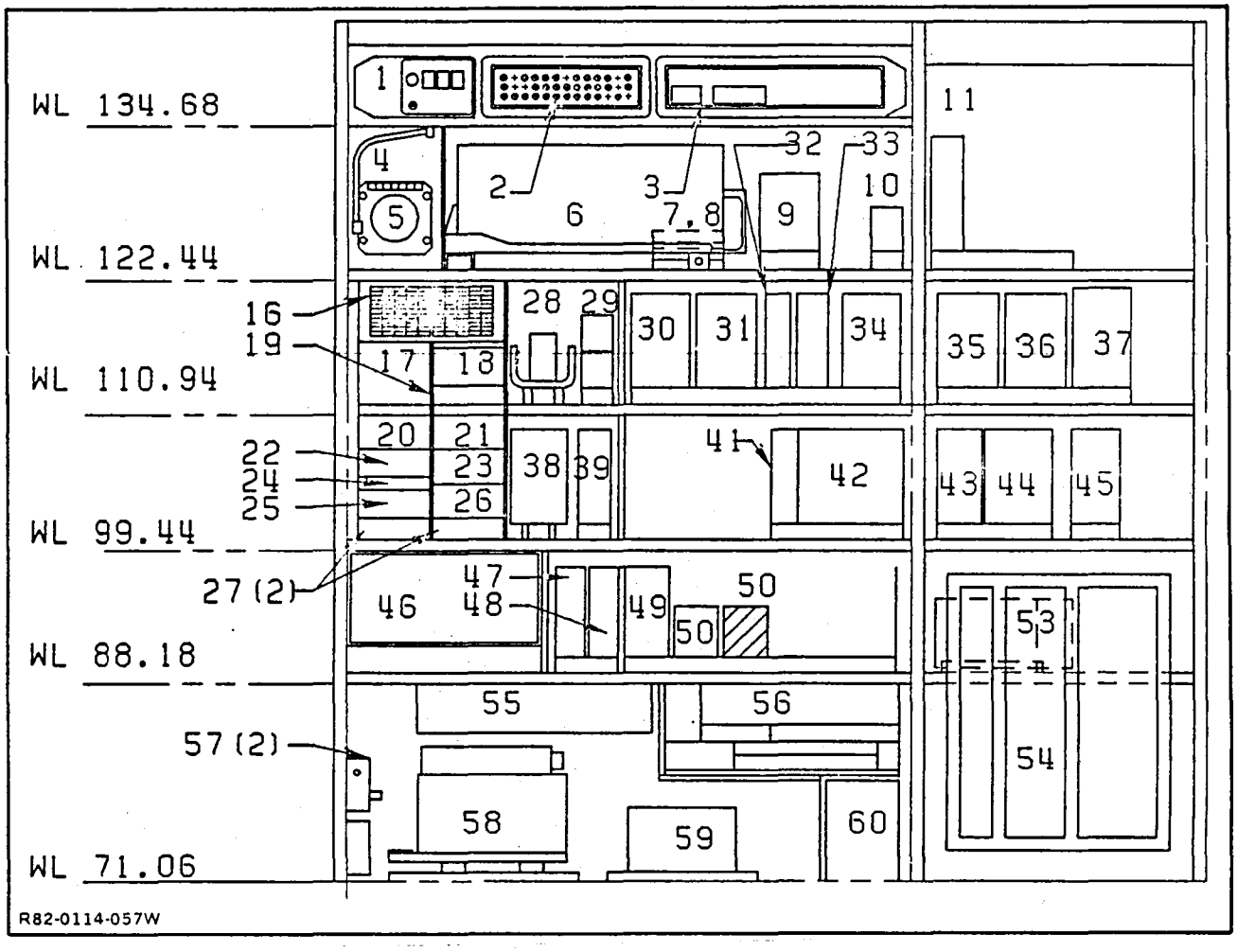


Figure 100 FBW Electronic Installation, R/H Side

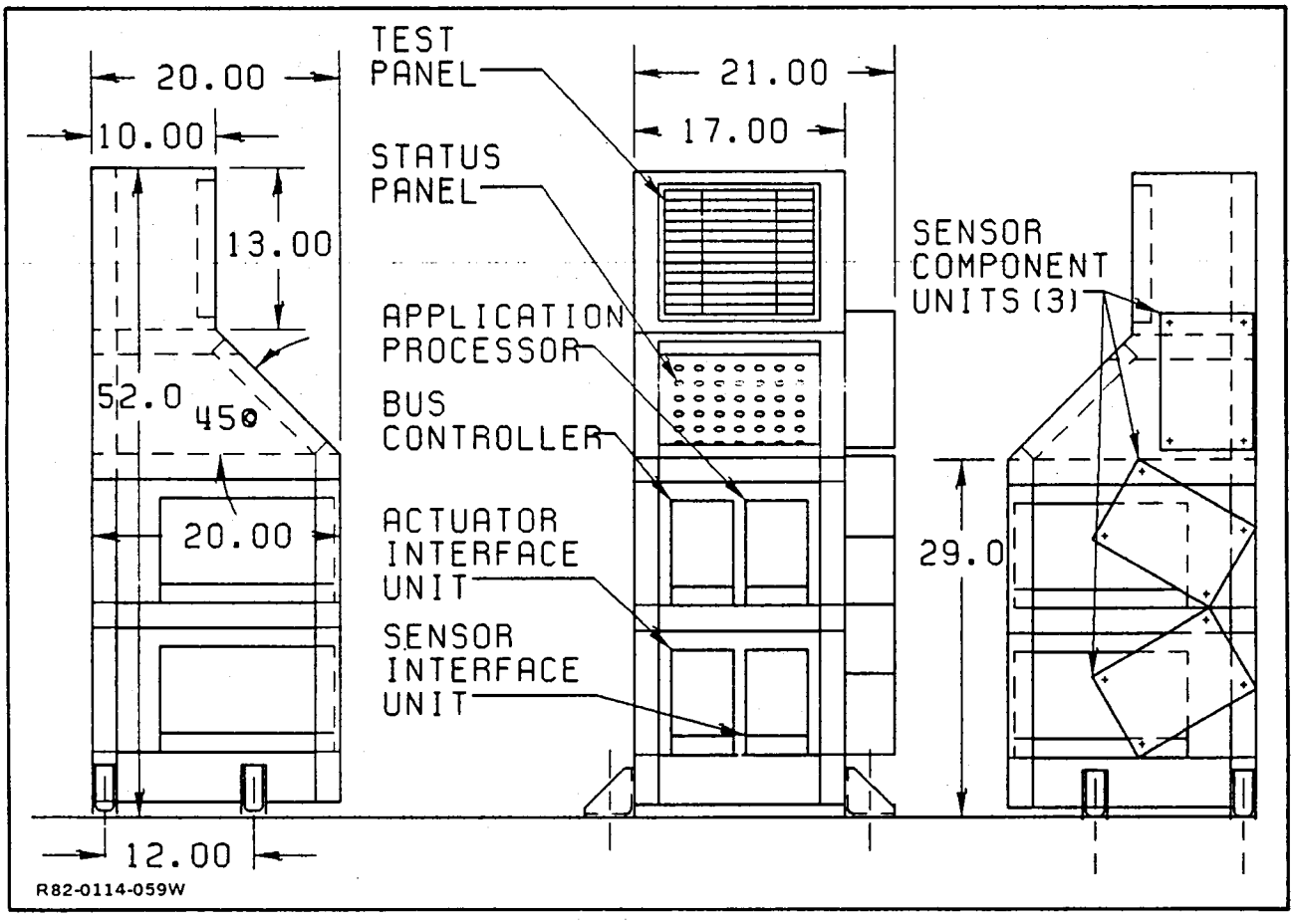


Figure 101 Fly-by-Wire Pallet

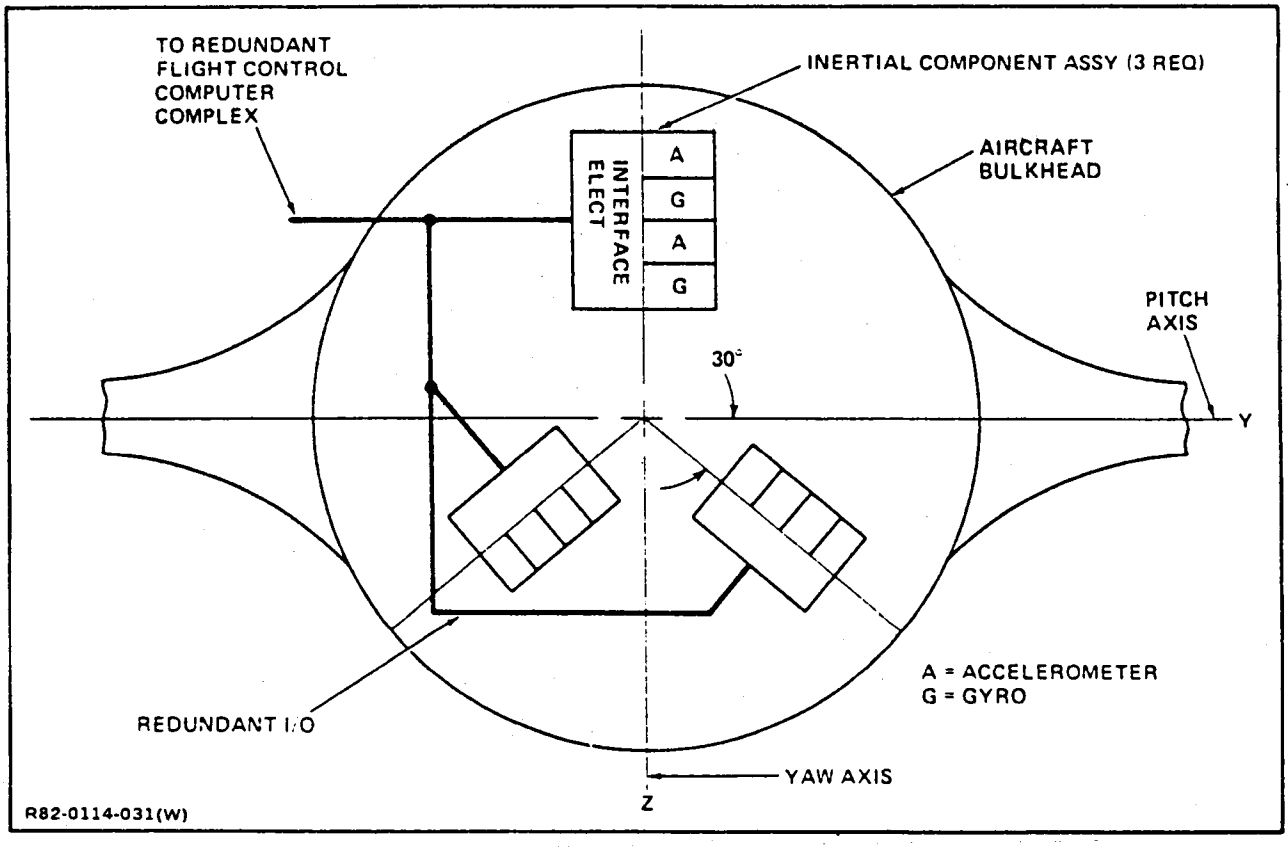


Figure 102 Inertial Subsystem Hardware Configuration

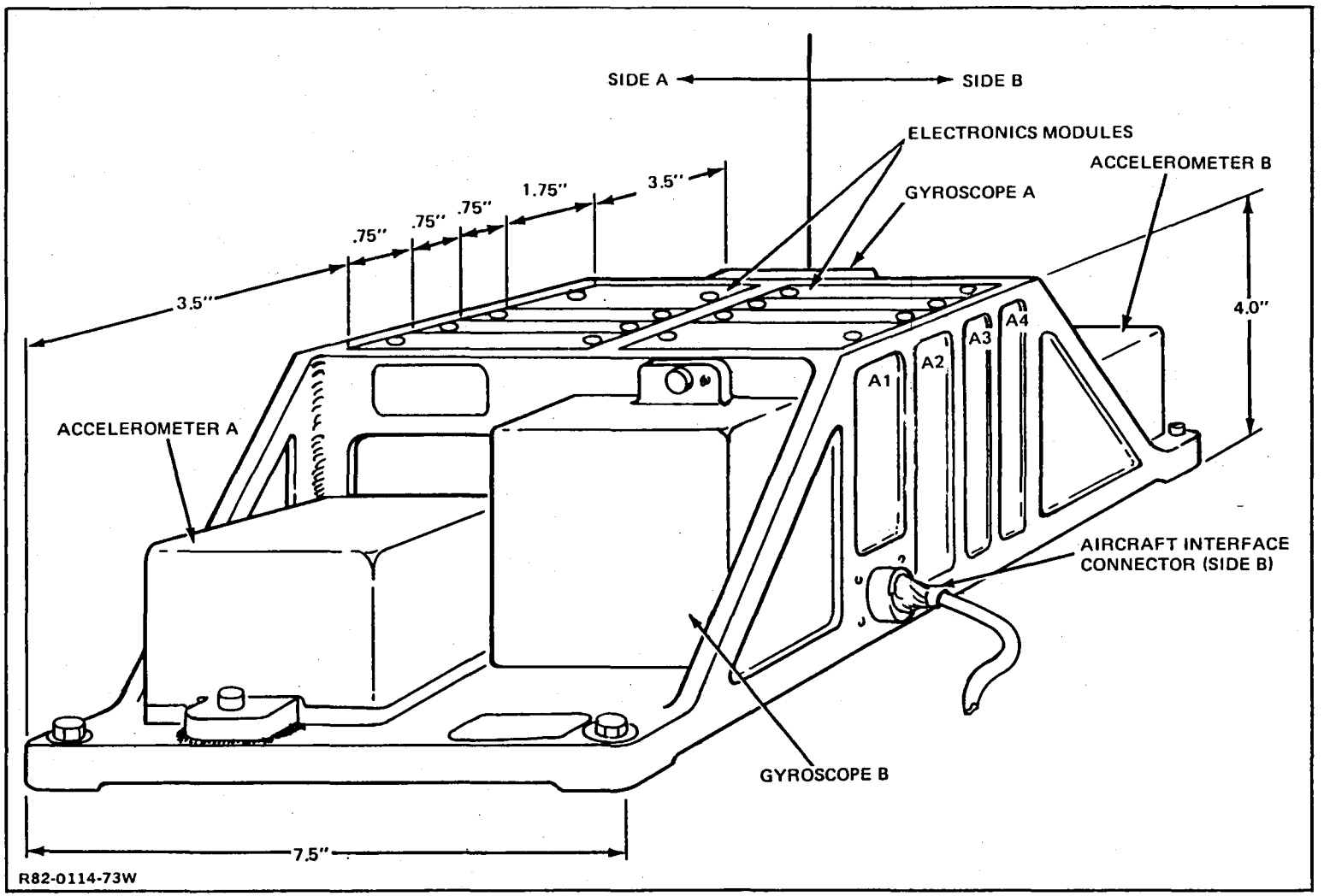


Figure 103 Inertial Component Assembly

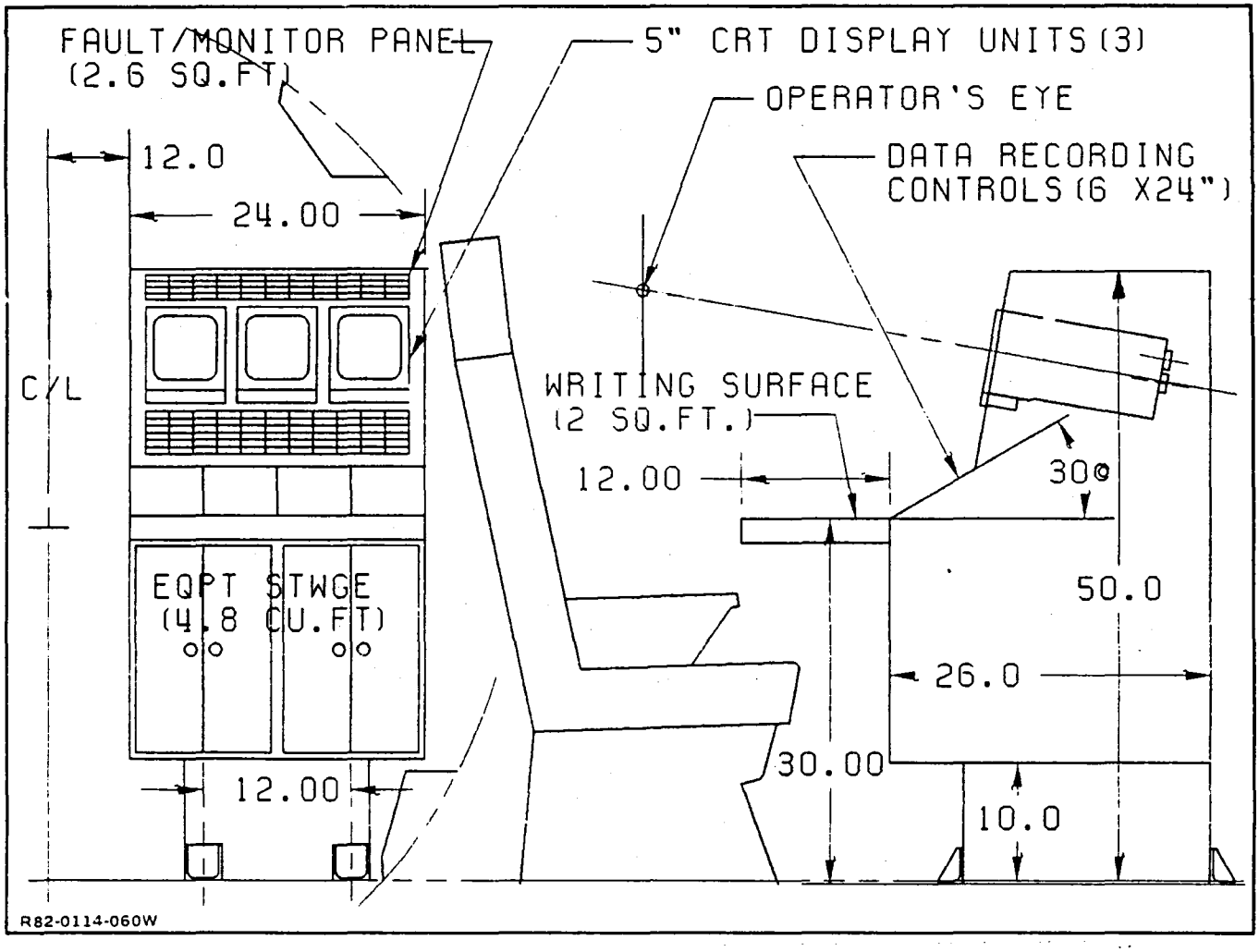


Figure 104 FBW Monitor/Work Station

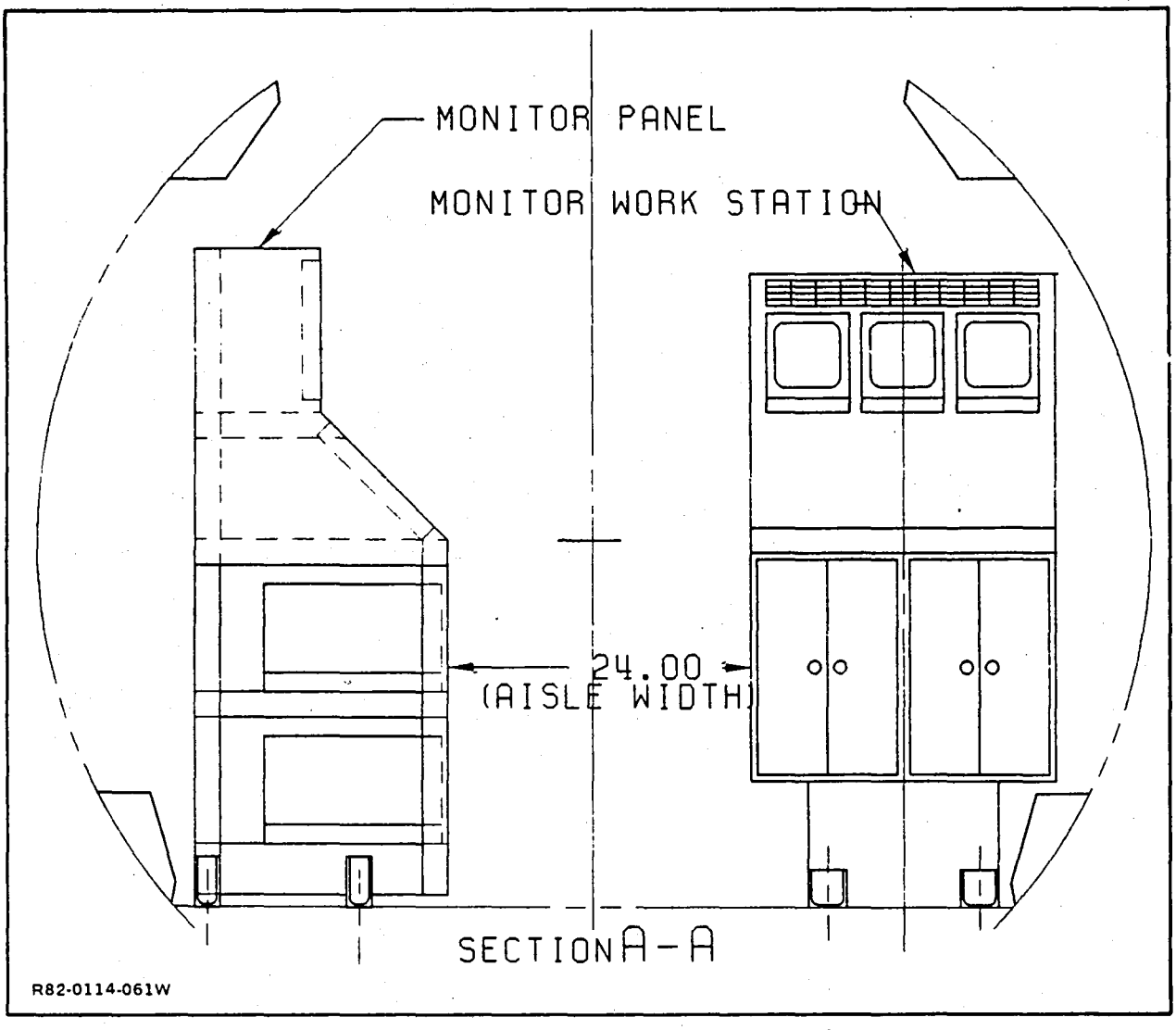


Figure 105 FBW Cross-Section, Looking Aft

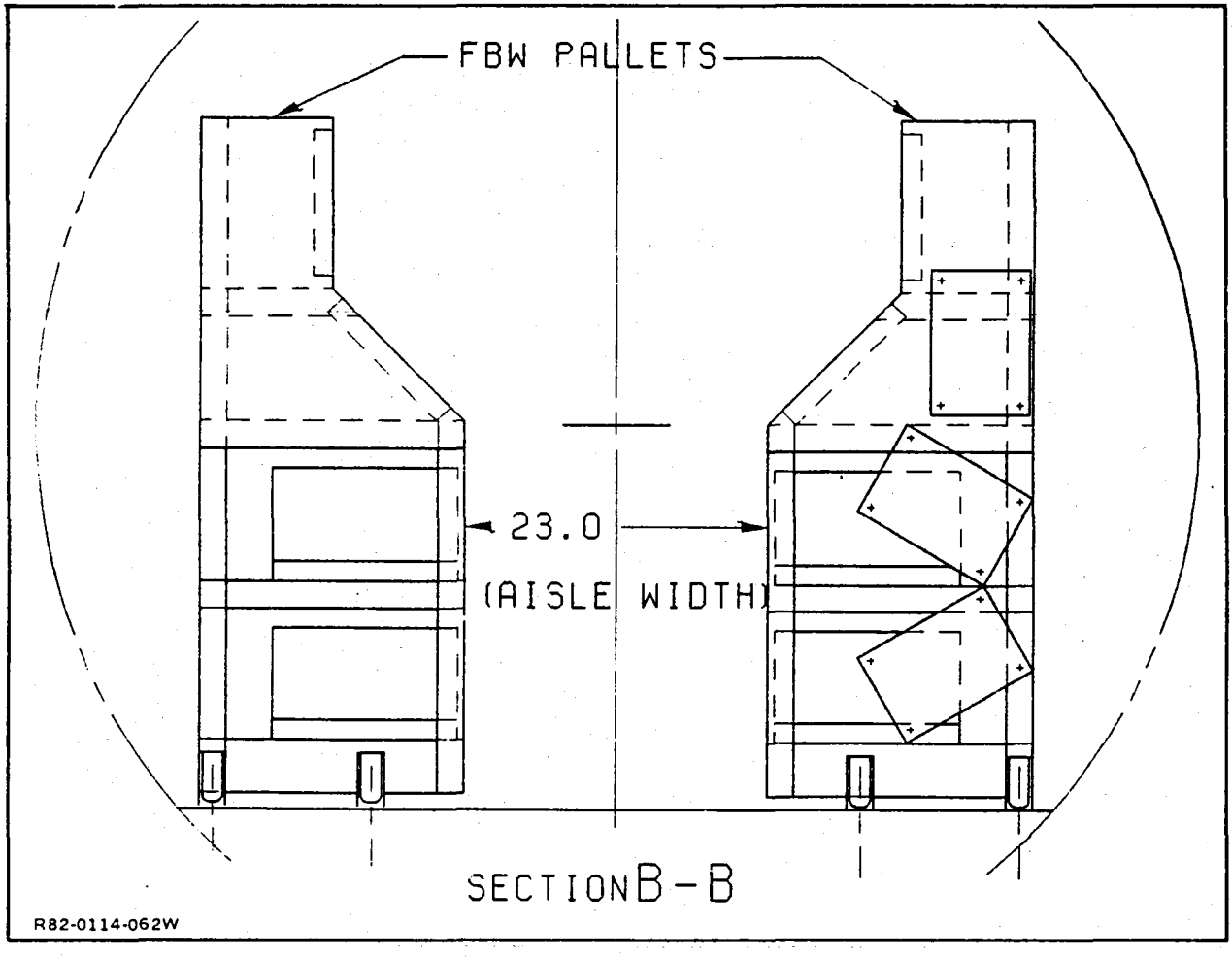


Figure 106 **Cabin Cross-Section, Looking Aft**

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS

INSTRUCTOR PILOT DISPLAYS		TYPE-P/N
*1.1	Flight Director Indicator (FDI) (HZ-6F)	Sperry 2590281-906
*1.2	Horizontal Situation Indicator (HSI) (RD-350M)	Sperry 4011046-901
1.3	Altimeter (Servo Driven)	Sperry 2594620-905
1.4	Vertical Speed Indicator (D6HL)	Teledyne SLZ9157-1
1.5	Standby Attitude Indicator (AI-804J/G)	Jet 501-1105-04
*1.6	Altimeter (Pneumatic)	IDC 570-23932-001
1.7	Mach/airspeed Indicator	IDC 575-25850-909
1.8	Radar Altimeter	Honeywell ID-1880/APN194(V)
1.9	Gyrosyn Compass (RMI) (C-63)	Sperry 1784460-655
1.10	Vertical Scale Engine Instr's	Hartman
1.10.1	Engine Pressure Ratio (EPR)	622-0-000-7
1.10.2	Turbine Gas Temp. (TGT)	623-0-000-8
1.10.3	% RPM HP	624-0-000-8
1.10.4	% RPM LP	621-0-000-8
1.10.5	Fuel Flow	684-0-000-7
1.10.6	Fuel Quantity	639-0-000-7
1.10.7	Oil Temp	625-0-000-7
1.10.8	Oil Press	626-0-000-7
1.11	Clock	Waltham A13A
1.12	Static Pressure Valve	Republic Mfg. Co. 11-254-8
1.13	Landing Gear control	Avionic Prod. 1159F20775
1.14	Angle of Attack Group	
1.14.1	Angle of Attack Ind.	United Control 966-0031-001
1.14.2	Indicator Light	Mstr Specialties 2224-1
1.14.3	AOA Selector	MS 24523-23
1.14.4	AOA Test/Reset Sw	MS 24523-27
*1.15	IP Instr Switches	
1.15.1	VG1, VG2,	Jayel Mk8 Series
1.15.2	NAV 1, NAV 2	Jayel Mk8 Series
1.15.3	Compass 1, Compass 2	Jayel Mk8 Series

* STA items removed

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

INSTRUCTOR PILOT DISPLAYS		TYPE-P/N
1.16	Fuel Qty Test Switch	W101PAB3W
1.17	Windshield Wiper Switch	ITL1-2
1.18	Windshield Wiper Control	GAC 1159F20750
1.19	Emerg. Battery SW/Lts	Mast. Specialties 90E
*1.20	Flight Director Mode Lts	
1.20.1	Loc/Rev Lt	Mast. Specialties 5000
1.20.2	G/S - Ext Lt.	Mast. Specialties 5000
*1.21	F/D Sensitivity Sw	
*1.22	Flight Director Info	Bendix 2806448
*1.23	Horizontal Situation Info	Bendix 2806448

IP AUXILIARY INSTRUMENT PANELS		TYPE-P/N
2.1	LH Skirt Panel	
*2.1.1	Mode Selector Sw (FDS)	Sperry 2589582-903
*2.1.2	Instrument Remote Controller	Sperry 4001939-901
*2.1.3	Flt. Display Mode sw	
2.1.4	Engine Sync Sw/Lts	Mast Specialties 90E
2.2	RW Skirt Panel	
2.2.1	Surface Position Indicator	Weston 521605
*2.2.2	Auto Pilot Trim Ind.	Weston 253694
*2.2.3	Ind. Light Assy (A/P Supervisory)	34-1020-1
*2.2.4	Mach Trim Sw.	512TS1-50
*2.2.5	Yaw Damp Sw.	512T1-S
2.2.6	Rudder Limit lt.	MS25041
2.2.7	Single Rudder Limit Lt.	MS25041

* STA items removed

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

IP AUXILIARY INSTRUMENT PANELS	TYPE-P/N
2.3 RH Console Assy	
2.3.1 Aux Hyd Pressure Ind	Glassco 1159SCH241-7
2.3.2 Utility Hyd Pressure Ind	Glassco 1159SCH241-5
2.3.3 Comp Hyd Pressure Ind	Glassco 1159SCH241-1
2.3.4 Flt. Hyd Pressure Ind	Glassco 1159SCH241-3
2.3.5 Wheel Brake Pressure Ind	AW2057AC01
2.3.6 Fuel Tank Temp	Weston 253685
2.3.7 Fuel Temp	Weston 260638
2.3.8 Free Air Temp	Weston 253686
2.3.9 Aux Hyd Pump Sw	
2.3.10 Utility Hyd Pump Sw	

IP CONTROL PANELS	TYPE-P/N
3.1 RH Console	
3.1.1 Emergency Landing Gear Ltl	Gac 159F10825
3.1.2 Aux DLC Panel	Gac C21A0355
3.1.3 Nose Wheel Steering Control	Gac C21G1101
3.1.4 Oxygen Regulator Control	Bendix MS22062
3.1.5 -	
3.1.6 Compass Control (C-11B)	Sperry 1775132-22
3.1.7 Circuit Breaker Panel	Gac C21A0260
3.1.8 ADC Air Supply Control	Gac 1159F20633
3.1.9 Aux Stabilizer Control	Gac -
3.1.10 Foot Air Outlet Control	Gac 1159AC20002
3.1.11 ICS Jacks	
3.1.12 Ldg Gear Emer Dump Valve	Gac 1159F20278
3.2 RH Fairing	
3.2.1 Master Warning Lts	Aero Avionics 704842
3.2.2 Cockpit Ltg Control	Gac C21A0299
3.2.3 ICS Speakers	Utah Elect. C35EC

* STA items removed

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

CENTER PEDESTAL		TYPE-P/N
4.1	Console	
*4.1.1	Mode Select Panel	Sperry 4008171
*4.1.2	CRT Keyboard	IBM MC65-0007-002
4.1.3	VHF Nav 1 & 2 Panel	Gables C-4661
4.1.4	TCN Control Panel	Hoffman C-9599A/ARN-117
4.1.5	VHF Control Panel	Collins 622-0356-002
4.1.6	INS CDU (LTN 51)	Litton 66350-04
4.1.7	ATC/MKR Panel	Gables G-4668
4.1.8	VHF Comm 1 & 2 Panel	Gables G-4660
*4.1.9	Data Entry Panel	Sperry 4019817
4.1.10	L/H Audio Sel Panel	Gac C21A0353-1
4.1.11	R/H Audio Sel Panel	Gac C21A0353-3
4.1.12	Any Select Switch	MS24523-22
*4.1.13	Stall Barrier Switch	MS24524-23
4.1.14	Rudder Trim Control	Gac 1159AV22221-1
4.1.15	Aileron Trim Control	Gac 1159AV22222-1
*4.1.16	Status Test Sw/Lts	Jayel 10620
*4.1.17	SP Instr Switches	Jayel 10620
4.2	FWD Control Pedestal	
4.2.1	Voice Recorder Panel	Collins 914F-1
4.2.2	Mode Selector Unit (Ins)	Litton 663570-03
*4.2.3	CRT Switches	Micro 13A6402-72
4.2.4	Park/Emerg. Brake	Gac 1159F20800
4.2.5	Gust Lock Lever	Gac 1159F20351
4.2.6	Ground Spoiler Hyd Press. Sw.	MS24659-23D
4.2.7	Antiskid Switch	MS24659-23D
*4.2.8	Inflight Thrust Reverse Sw.	Micro 5ET17-2-F
4.2.9	-	
4.2.10	Main Gear Speed Brake Lt	Gac C21A073-5
4.2.11	Main Gear Speed Brake Sw.	Micro 5ET17-2-F
4.2.12	Eng. Temp Control Sw.	GS8363CJ3-1
4.2.13	Longitudinal Trim Wheel	Hansen Lynn 1159F20351
*4.2.14	DLC (Flap) Lever	Gac C21F1120
4.2.15	Stab Trim Sw.	

* STA item removed

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

CENTER PEDESTAL		TYPE-P/N
4.3	Power Control Head	Hansen Lynn 1159SCF100
4.3.1	Thrust Levers	
4.3.2	Reverse Thrust Levers	
4.3.3	High Pressure Fuel Cock Levers	
4.3.4	Friction Control Lever	
4.3.5	Thrust Reverser Disable Sw.	

SP INSTRUMENT PANEL		TYPE-P/N
*5.1	Attitude Director Ind (LM)	NASA MOD C21F125
*5.2	Horizontal Situation Ind (HSI) (RD-350M)	Sperry 4011046-901
*5.3	Alpha, Mach, IAS, Vert Scale Ind	Malwin 1660-1
*5.4	Mach/IAS Ind	Sperry 2594621-903
*5.5	V/S, Alt, Rad Alt, VSI	Malwin 1661-1
5.6	Altimeter (Servo Driven)	Sperry 2594620-905
*5.7	CRT Display Unit	IBM MC615-0006-0002
5.8	Accelerometer	NASA Mod type MA-1
*5.9	Surface Position Ind (Orbiter)	Weston 521606
*5.10	Angle of Attack (Orbiter)	Rosemount 30R-1
*5.11	Angle of Sideslip (Orbiter)	Rosemount 30R-2
5.12	Clocl	Waltham A13A
*5.13	Data Select Sw.	Grayhill 44-D-30-01-2-AJN
*5.14	Display Power Sw.	Micro weAT402/T2
*5.15	LDG Gear Position Ind (ORBITER)	Gac C21A0351-3
*5.16	LDG Gear Arm & Dwn Sw/Lts	
*5.17	ADI Scale Sws	Micro 13AT402-T2
*5.18	HSI Select Sws.	Micro 13AT402-T2
*5.19	Air Data Select Sw.	Micro 13AT402-T2

* STA items removed

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

SP INSTRUMENT PANEL		TYPE-P/N
#5.20	Flight Director Info	Bendix 2806448
#5.21	Horizontal Situation Info	Bendix 2806448
#5.22	Mach/Airspeed Indicator	IDC 575-25850-909
#5.23	Gyrosyn Compass (RMI) (C-6E)	Sperry 1784460-655
#5.24	Vertical Speed Indicator (D6HL)	Teledyne SLZ 9157-1
#5.25	Radar Altimeter	Honeywell ID-1880/APN194(V)
#5.26	Caution Advisory	Bendix 2806448
#5.27	Caution Advisory	Bendix 2806448

SP CONTROL PANELS		TYPE-P/N
6.1	LH Console	
6.1.1	Cockpit Ltg Panel	Gac C21A0298
6.1.2	Oxygen Regulator Control	Bendix MS22062
*6.1.3	Speed Brake Control (Orbiter)	Gac C21A0293
*6.1.4	Instrument Remote Controller	Sperry 4001939-901
6.1.5	Spare Camp Stowage	
*6.1.6	Body Flap Sw	
*6.1.7	Trim Yaw Sw	
6.1.8	-	
6.1.9	-	
6.1.10	Oxygen Shut Off Control	Gac C21E1002
6.1.11	Aux Hyd Pump Sw.	
6.1.12	Foot Air Outlet Control	Gac 1159AC20002
6.1.13	ICS Jacks	
6.2	LH Fairing	
*6.2.1	Controller Power Sw	
6.2.2	Oxygen Pressure Ind.	ANG011-1B
6.2.3	Circuit Breaker Panel	GAC C21A0261
6.2.4	ICS Speaker	Utah Elect. C35EC
6.3	Rotational Hand Controller (LM)	NASA Mod C21F1109

* STA items removed
# FBW items added

TABLE 16

COCKPIT INSTRUMENTS & DISPLAYS (CONT'D)

GLARESHILED PANEL		TYPE-P/N
*7.1	Flt Control Sw/Lts (Orbiter)	Jayel 10620
7.2	Master Warning Lts	Mstr Specialties 90E
*7.3	Event Sequence (Orbiter)	GAC C21A0267
*7.4	Touch Down Lt	Mstr Specialties 90K
*7.5	Emergency Control Panel	GAC C21A0268
*7.6	Status Display	Sperry C21F108
7.7	-	
*7.8	STA Warning Lts	Mstr Specialties 90K
7.9	Marker Beacon Lts	MS 25041

MISCELLANEOUS		TYPE-P/N
8.1	Standby Compass	Airpath CB-2100-T6-D
8.2	Lower Overhead Panel	GAC C21A0276
8.3	Center Overhead Panel	GAC C21A0274
8.4	Upper Overhead Panel	GAC 1159F20777
8.5	IP Control Wheel	GAC C21A0280
8.6	Flt Hyd Shutoff Valve	GAC 1159F20840

* STA items removed

TABLE 17

ELECTRONIC RACK INSTALLATION

	NOMENCLATURE	SELLER/PART NO.
1.	Vestibule Light Control	
2.	Auxiliary Circuit Breaker Panel	
3.	Static Pressure Select Valve	C21F1203
4.	Map Light	
5.	Weather Radar Scope	RCA MI-585011-2
6.	Inertial Navigation Unit	LITTON 663450-8
7.	Engine Oil Temp. Unit	HARTMAN 625-0-0007
8.	Engine Oil Press Unit	HARTMAN 626-0-0007
9.	Inertial Navigation Battery	LITTON 500012-02
10.	Marker Beacon Receiver	COLLINS 522-2996-011
11.	Gyro Horizon Power Supply	JET 501-1075-02
*12.	Flight Director Roll Axis Comp.	SPERRY 2588145-907
*13.	Flight Director Pitch Axis Comp.	SPERRY 2588146-907
*14.	Rate of Turn Rack	SPERRY 2588424-906
*15.	Pitch, Yaw/Roll Rate Gyro	SPERRY -4019811, -4019812
16.	Master Caution Panel	
17.	Gyrosyn Compass (RMI)	SPERRY 1784460-659
18.		
19.		
20.	MSBLS Power Control Panel	
21.	Compass Controller	
22.	ICS Panel	
23.	Flight Recorder Encoder	
24.	Blank	
25.	Blank	
26.	Oxygen Control Panel	
27.	Remote Compass XMTTR	SPERRY 2586257-1
28.	Inverter (800 HZ)	ABBOTT 22843
29.	Angle of Attack Cmptr. (2)	UNITED CONTROL 965-0041-005
30.	VHF Comm. Trans.	COLLINS 522-4089-201
31.	VHF Comm. Trans.	COLLINS 522-4089-201
32.	Compass Amplifier	SPERRY 614937-10
33.	Compass Amplifier	SPERRY 614937-10
34.	Air Data Computer	SPERRY 2593200-910
35.	VHF Nav. Receiver	COLLINS 522-4280-101
36.	VHF Nav. Receiver	COLLINS 522-4280-101

TABLE 17

ELECTRONIC RACK INSTALLATION (CONT'D)

	NOMENCLATURE	SELLER/PART NO.
37.	DME	COLLINS 522-4209-012
38.	Weather Radar Receiver/Transmitter	RCA MI-585009
39.	Audio Amplifier	COLLINS 522-4538-002
*40.	Status Panel Electron Unit	SPERRY 4021785
41.	Tacan Conv. Signal Data	HOFFMAN CV 31881-117
42.	Tacan Rcvr./Xmttr.	HOFFMAN RT-1127/ARN-84(V)
43.	RF Assy (MSBLS)	
44.	Decoder Rcvr. (MSBLS)	
45.	A.T.C. Transponder	
46.	Jump Seat	
47.	Anti-Skid Control Box	
48.	Cabin Pressure XDCR	
49.	Air Data Computer	
50.	Radar Altimeter Rcvr./Xmttr.	
#50.	Radar altimeter Rcvr./Xmttr.	
*51.	Stability Augmentation Compt.	
*52.	Display Electric Unit (DEC)	
53.	Transformer/Rectifier	
54.	Magnetic Tape Recorder	
55.		
56.		
57.		
58.		
59.		
60.		

* Delete from STA for FBW
\# Add for FBW

APPENDIX I

MODIFIED STA FLIGHT CONTROL SYSTEM

1. General Description of STA Flight Control Systems

The primary flight control systems of the STA are the Longitudinal (elevators, pitch control), Lateral (ailerons and flaperons, roll control), and Directional (rudder, yaw control) systems. They are hydraulically powered and boosted systems wherein the pilot, through mechanical linkages, pushrods, and cables, actuates dual tandem hydraulic boost actuators to move the control surfaces. The dual tandem hydraulic actuators receive hydraulic power from two independent pressure sources, the Flight and the Combined Hydraulic Systems. The Combined Hydraulic System maintains a pressure of 3000 PSI during landings and take-offs, but switches to 1500 PSI during normal flight conditions upon retracton of landing gear and flaps. Loss of system pressure of one hydraulic system has no effect on operation of the flight controls. If either system fails, the other automatically shifts to 3000 PSI to maintain actuator load capacity. In the event of total pressure loss to both hydraulic system, the controls revert to manual operation. The ailerons, flapersons, elevators, and rudder flight control surfaces are mass balanced to prevent flutter in the manual mode of operation.

Lift augmentation for take-off and landing during the non-simulation mode of flight is provided by flaps and flaperons on each wing. During the simulation mode of flight, these control surfaces are used to simulate orbiter flight characteristics. The flaperons also provide roll control and operate in conjunction with the Lateral Control System functioning simultaneously with both systems. The flap and flaperon control surfaces extend along the trailing edge of the wing from the fuselage to the ailerons. Control is accomplished in the non-simulation mode by the DLC/Flap Handle. Both sets of control surfaces operate through a series of pushrods, cables, and cranks to the flap and flaperon hydraulic power actuators. Both flap and flaperon actuators are a tandem arrangement of two double acting balanced cylinders supplied by two separate hydraulic systems. The flaps, left flaperon, or right flaperon, may be isolated manually by the pilot from the aircraft hydraulic system in the event of a malfunction; when this occurs, the control surface assumes trail position.

A movable stabilizer compensates (trims for nose tuck-in) when the flaps are lowered to their takeoff or landing position of -20^{o} during the nonsimulation mode of flight. The stabilizer has the capability of moving form 0^{o} to 2^{o} leading edge down. Its only control mode is for flap trim compensation.

The STA Trim Control Systems provide for trim about all three axes. Manual trim control is accomplished by moving control wheels mounted on the Control Pedestal, or Center Console, in a position corresponding to the respective trim axis. Cable operated mechanical screwjack actuators are used to provide trim surface displacements in both the lateral and directional control systems. The lateral trim actuator drives a trim tab on the left aileron. The directional trim actuator varies the neutral position of the directional system by displacing the rudder actuator, driving the rudder to the desired trim position. The longitudinal trim system can be trimmed manually, or by means of elevator trim switches, located in the Instructor Pilot's control wheel. Longitudinal trim is accomplished manually by rotating the trim wheel and driving a cable drum or electrically by driving a servo motor. The servo motor responds to trim switch inputs and drives the cable drum, which is common to both manual and electrical operation. Operation from either source transmits motion by a cable control to drive both left and right elevator trim tabs simultaneously.

2. General Description of Modifications

Basically, the FBW Modifications involve removal of the aircraft cable and trim systems and the addition of electrically controlled actuators to provide inputs to the surface controls. The co-pilot control wheel and pedals are modified to provide appropriate artifical feel devices and transducer pick-offs for the computer signals.

The baseline STA cockpit retains the interesting potential for evaluation of a control wheel vs. hand controller for piloting a transport type aircraft. Alternatively, the cockpit could be configured with dual FBW hand controllers, if so desired.

3. STA Longitudinal Control System

Longitudinal control is provided by means of conventional elevators. Control in the STA is accomplished in the non-simulation mode by fore and aft motion of the Instructor Pilot's control column, and in the manual simulation mode through the Simulation Pilot's Rational Hand Controller (Figure 107). Motion of the control column is transmitted through

mechanical linkages to the hydraulic power boost mechanism in the tail section. The rotational hand controller is electrically connected to the control system, through the DAS. The elevator actuator is a tandem double acting balanced cylinder, moving body type, identical to the left aileron actuator. Trim is accomplished by means of elevator trim tabs either manually, or electrically. The horizontal stabilizer is also movable for trim purposes.

4. FBW Longitudinal Control System

The longitudinal control system can be revised to a FBW configuration, from the existing GII-STA mechanical input, hydraulically boosted system, as shown in Figure 108. This will be accomplished by the following:

1) Remove the connecting elements between the pilots control column and the boost actuator valve input as shown in Figure 108.

2) Revise the reaction point for the existing elevator boost actuator, converting it to a fully powered configuration.

3) Modify the existing actuator boost valve from the "overlap" design to a "line to line" configuration, increasing the resolution and frequency response of this system.

4) Install two dual tandem electro-hydraulic command actuators to replace the manual inputs to the power actuator control valve. The outputs of each dual tandem actuator will be force summed, i.e.; both pushing on the same fail-safe crank to displace the elevator actuator valve in the commanded direction.

5) Modify the co-pilot control column for FBW with a multi-element transducer (or transducers) to provide command inputs to the computers, and connect the control column to a 'q' sensitive artifical feel system that will provide the pilot with a simulated force as required by the flight condition. A column damper will be incorporated to cater to the system hardware dynamics, and the column will be mass balanced.

6) Remove the trim tab control system components with the trim tabs grounded at the elevator. Series trim is incorporated through a trim wheel on the control wheel.

5. STA Lateral Control System

Lateral control of the aircraft is provided by both ailerons and flaperons on each wing. The flaperons also operate in conjunction with the Flap/Direct Lift Control System and function collectively with both systems. Control in the STA is accomplished in the nonsimulation mode by rotating the Instructor Pilot's control wheel, and in the manual simulation mode through the Simulation Pilot's Rotational Hand Controller, Figure 109. Motion of the control wheel is transmitted through mechanical linkages to the hydraulic power boost mechanism of the ailerons and flaperon power actuators. The rotational hand controller is electrically connected to the control system, through the DAS. Both aileron and flaperon actuators are dual tandem double acting balanced cylinders supplied by two separate hydraulic systems. The aileron actuator is a moving body type, while the flaperon actuator is a stationary body type. Trim is accomplished by means of a tab on the left aileron.

6. FBW Lateral Control System

The lateral control system can be revised to a FBW configuration, from the existing GII mechanical input, hydraulically boosted system, as shown in Figure 110. This is accomplished by the following:

1) Remove the connecting elements between the pilot control wheel output and the wing cable system.

2) Revise the reaction points for each aileron actuator converting it to a fully powered configuration. The existing actuator valves will be modified from 'overlap' to 'line to line', increasing the resolution and frequency response of the ailerons.

3) Install two dual tandem force summed command actuators, one on each side of aircraft center line, to replace the manual inputs to the wing cable.

4) Modify the co-pilot's control column with a multi element transducer (or transducers) to provide inputs to the computer and connect an artificial feel system and damper. The trim tab inputs will be removed and the trim tab will be deactivated by grounding it to the aileron. Series trim is incorporated through the GII lateral trim wheel driving an input transducer.

5) Add a hand controller at the pilot's station.

7. STA Flap/Direct Lift Control System

The Flap/Direct Lift Control (DLC) System includes both flap and flaperon control surfaces and is utilized during all modes of flight. The flap system provides lift augmentation for take-off and landing during the non-simulation mode of flight. The DLC system controls aircraft attitude and motion to simulate Orbiter visibility and acceleration changes associated with angle-of-attack changes, wind gusts, maneuvers, and ground effects realized during final stages of approach, in the simulation mode of flight.

The flaperons also operate in conjunction with the Lateral Control System and function simultaneously with both systems through a mixing linkage.

In the non-simulation mode, the flaps and flaperons are operated by the flap system and are controlled manually by the DLC/FLAP handle, located on the control pedestal. The handle is mechanically connected to an input bungee containing the flap up and down switches, which control the DLC trim actuator. The actuator, through mechanical linkages, operates the control valves on the flap and flaperon servo actuators which position their respective control surfaces. As the DLC trim actuator moves, the input bungee will be repositioned until the control surface position corresponds to DLC/FLAP handle input. At this time the bungee will be in its neutral position with both control switches grounded.

8. FBW Flap/Direct Lift system

The high lift system will be modified for FBW operation. A flap position electrical trim actuator (identical to the LH side) will be added to the RH flap linkage. This will replace the existing cable run which originates in the LH flap linkage, goes to the cockpit pedestal, and then, to the RH wing flap input linkage.

The DLC servo actuators will be maintained to provide 'quick acting' DLC, if required.

9. STA Directional Control System

Directional control of the aircraft is provided by means of a single rudder. Control is initiated by moving either pair of dual rudder pedals, Figure 111. Motion of the Instructor Pilot's pedals is transmitted through mechanical linkage to the power actuator located in the tail section. The Simulation Pilot's pedals are electrically connected, through the DAS, to

the power actuator. Each set of pedals also incorporate a bungee for artificial feel. Maximum rudder travel is 22° left and 22° right. The dual tandem hydraulic power actuator consists of two double acting balanced cylinders supplied by two separate hydraulic systems. The actuator also includes a series mode yaw damper, autopilot control, DAS control, and an automatic feature that limits rudder hinge moment. In the event this force is reached, a RUDDER LIMIT light (green) on the Instructor Pilot's right Skirt Panel will illuminate. The rudder does not utilize a trim tab but is displaced to a new neutral position for trim corrections.

10. FBW Directional Control system

The directional control system will be revised to a FBW configuration, as shown in Figure 112. This is accomplished by the following:

1) Remove the mechanical elements between the pilots rudder pedals and the rudder actuator valve input.

2) Incorporate two force summed dual tandem command actuators to replace the manual input actuator valve.

3) Modify the pilot's rudder pedals so that rudder pedal motions signal 2 multi-element transducers to provide inputs to the computer and connect an artificial feel system and damper to the pedals. The parallel trim system will be removed. Series trim is incorporated thru the GII directional trim wheel driving an input transducer.

11. Servo Actuators

The force summed dual tandem servo actuator configuration is identical for all three primary control systems. Each actuator of the pair is identical to the other and uses a direct drive electrohydraulic valve.

One dual tandem servo actuator is powered by the existing Flight and Combined systems each in a different chamber. The other dual tandem servo actuator is powerd by a new, (third) servo hydraulic system described below. For normal operation only one half of this actuator is powered (one chamber). If either or both primary hydraulic systems are lost (Flight and/or Combined), the other chamber is powered thru the servo hydraulic system. Further study may indicate that a fourth hydraulic system (Standby) may be needed. This system could then power the standby half of the servo actuator as required in lieu of the servo hydraulic system.

In the event both hydraulic systems are lost on the GII, the pilot can control the aircraft manually with no switching on his part. Since manual reversion is a 'get home' control, the control forces are high. For the FBW configuration, when the flight and combined hydraulic system are lost, the FBW servo actuator can control the surfaces. Electromechanical actuators can be substituted for the hydraulic units when they become available.

12. Electromechanical Actuation Systems

It is recommended that electromechanical actuation systems (EMAS) be considered and to be potentially phased into the program on an axis by axis basis. It is expected that EMAS could be incorporated into all flight control actuator applications by 1988 to 1989. Prior efforts described in the actuation survey section of this report defines the specific configurations and designs for each control surface application. We expect that most of the EMAS for the Gulfstream would be rotary hinge line designs. The rudder and elevator units would undoubtedly be force summed, each having two motors with each motor being dual magnetic torque summed motors. Each actuator could then be considered quadruple redundant, at least to the gear box section where it would be dual. Clutches would isolate failed or jammed motors and perhaps part of the mechanical gearing. Figure 113 shows a typical installation of an EMAS in the elevator axis of the longitudinal control system of the FBW Gulfstream.

13. Control Surface Indication

The control Surface Position Indication System (SPI) provides the Instructor Pilot with visual indications of the positions of the following flight control surfaces: left and right flaperons, left and right flaps, horizontal stabilizer, left and right side-force generators, elevator, and rudder. The system also provides control surface position inputs to the Digital Avionics System (DAS) for use during the simulation (Orbiter) mode of flight.

In addition to the SPI, the Control Surface Indication System includes seven synchro transmitters and two linear voltage differential transmitters, for sensing control surface positions, and seven Synchro/DC Converters for converting the synchro transmitter outputs to DC drive signals for the SPI.

14. Angle of Attack System

A redundant Angle of Attack system is installed in the aircraft consisting of:

A. An Indicator to show the angle of the aircraft in relation to stall.

B. Two Shaker Motors, used to vibrate the Instructor Pilot's Control Column, and an aural warning, which alerts the crew of an impending stall.

C. A dual control Stall Barrier system (Stick Pusher), used to prevent a stall by forcing the Instructor Pilot's Control Column forward when the crew fails to respond to the indicator, shaker motor vibration, or aural warning.

If the aircraft nears stall, and Stall Barrier operation is called for, hydraulic valves are energized open, porting hydraulic fluid to a cylinder that pushes the Elevator down and the Instructor Pilot's Control Column forward. The Instructor Pilot can overcome this force by exerting an approximate 55 pound pull on the column if the 1500 PSI hydraulic system is engaged, and 72 pound pull with 3000 PSI system engaged.

Either system can deliver information to the Angle of Attack Indicator located on Instructor Pilot's Flight Instrument Panel. This is dependent upon the position of the Angle of Attack Selector Switch located adjacent to the indicator and selected by the crew.

15. Hydraulic Power System

The Gulfstream II STA (see Figure 114) has a dual-compensated (1500/3000 psi) normal hydraulic power system which includes the Combined (sys. No. 1) and the Flight hydraulic power system (system No. 2). The hydraulic power system is sub-divided into five systems as follows:

A. Combined - 1500/300 $\pm$ 50 @ zero flow
2900 $\pm$ 50 @ full flow

B. Flight - 1500/3000 $\pm$ 50 @ zero flow
2900 $\pm$ 50 @ full flow

C. Utility - 2900 $\pm$ 50 psi @ max. flow
3000 $\pm$ 50 @ zero flow

D. Auxiliary - 2950 ± 50 psi @ max. flow
3050 ± 50 @ zero flow

E. Emergency - 3000 psi (Nitrogen @ 70°F)

The hydraulic system is designed for use with Hyjet IV hydraulic fluid approved alternate fluids, and for operation temperatures from -54° to +107°C. (-65° to 225°F).

The Combined hydraulic system supplies 3000 psi, during takeoffs and landings to operate the flight controls and the landing gear stall barrier, wing flaps, wheel brakes, nose wheel steering, ground spoilers, thrust reversers and windshield wipers. During flight, the Combined hydraulic system supplies 1500 psi to operate the elevators, stall barrier, ailerons, rudder and speed brake/flight spoilers. The pressure compensation of 1500 or 3000 psi is accomplished by a series of electronically controlled switches which energize the engine pump solenoid.

For ground test and check-out procedures with the use of an external hydraulic rig, the Combined system is normally operated at 3000 psi.

The Flight system supplies 1500 psi to operate the flight controls of the aircraft. The only time the Flight system is compensated to 3000 psi is during Combined system failure (or when the right engine is started first). During a Combined system failure, Flight system pressure, at 3000 psi, is also available to power the hydraulic motor pump of the Utility system.

For ground test and check-out procedures with the use of an external hydraulic rig, the Flight system is also operated at 3000 psi.

In the event of a Combined system failure, other than hydraulic fluid loss, the Utility system supplies 3000 psi to operate the following sub-systems of the aircraft: stall barrier, landing gear, wing flaps, wheel brakes, nose wheel steering, ground spoilers, thrust reversers, and wind shield wipers. The Utility system includes a hydraulic motor-driven pump, the motor using flight system pressure to operate the pump, which in turn pressurizes combined system fluid to operate the sub-systems. During flight, with the Combined system failed, the Utility system is activated only when the landing gear handle, and/or the flap handle is moved to the down position.

The Auxiliary system supplies 3000 psi to operate the following sub-systems of the aircraft: auxiliary wing flaps, auxiliary brakes, park and emergency brakes, (using an accumulator), ground spoilers, and landing gear doors (for ground service). The Auxiliary system, with its pressure reduced to 1500 psi, also operates the main entrance door.

For ground test only, the Auxiliary system can also operate the landing gear.

The Emergency pneumatic system supplies 3000 psi for emergency extension of the landing gear only.

The Shuttle Training Aircraft (STA) and the Gulfstream II Aircraft Hydraulic Power Systems are identical, except for the following modifications to the STA (Figure 115):

A. The Combined Hydraulic System supplies 3000 PSI, during takeoffs and landings, to operate the flight controls, the landing gear, stall barrier, wheel brakes, nose wheel steering, thrust reversers, and windshield wipers. During ferry flight, the Combined Hydraulic System supplies 1500 PSI to operate elevator, ailerons, flaperons, flaps, and rudder. In the Simulation and Non-simulation Modes, the Combined Hydraulic System supplies 3000 PSI to operate the flight controls and landing gear, thrust reversers, side force generators, and stabilizer trim control.

B. The Flight System supplies 1500 PSI to operate the flight controls of the aircraft; namely, elevator, rudder, ailerons, flaperons, and flaps.

16. FBW Hydraulic System

The FBW configured GII will require a third hydraulic system to ensure flight control system safety. This additional system will allow this aircraft to meet FAR 25 requirements.

This third hydraulic system, identified as the Servo Hydraulic System, Figure 114, is dedicated to the FBW servo actuators only.

This Servo Hydraulic system will be completely independent of the existing systems (Flight and Combined). An electrically driven hydraulic pump will be installed to power this added system. The Servo system will power both halves of one of the added servo actuators, for each control axis, as per the flight control system hydraulic power requirements.

If ongoing studies indicate that a fourth system (Standby) is necessary, it would power the standby chamber of the actuator as required.

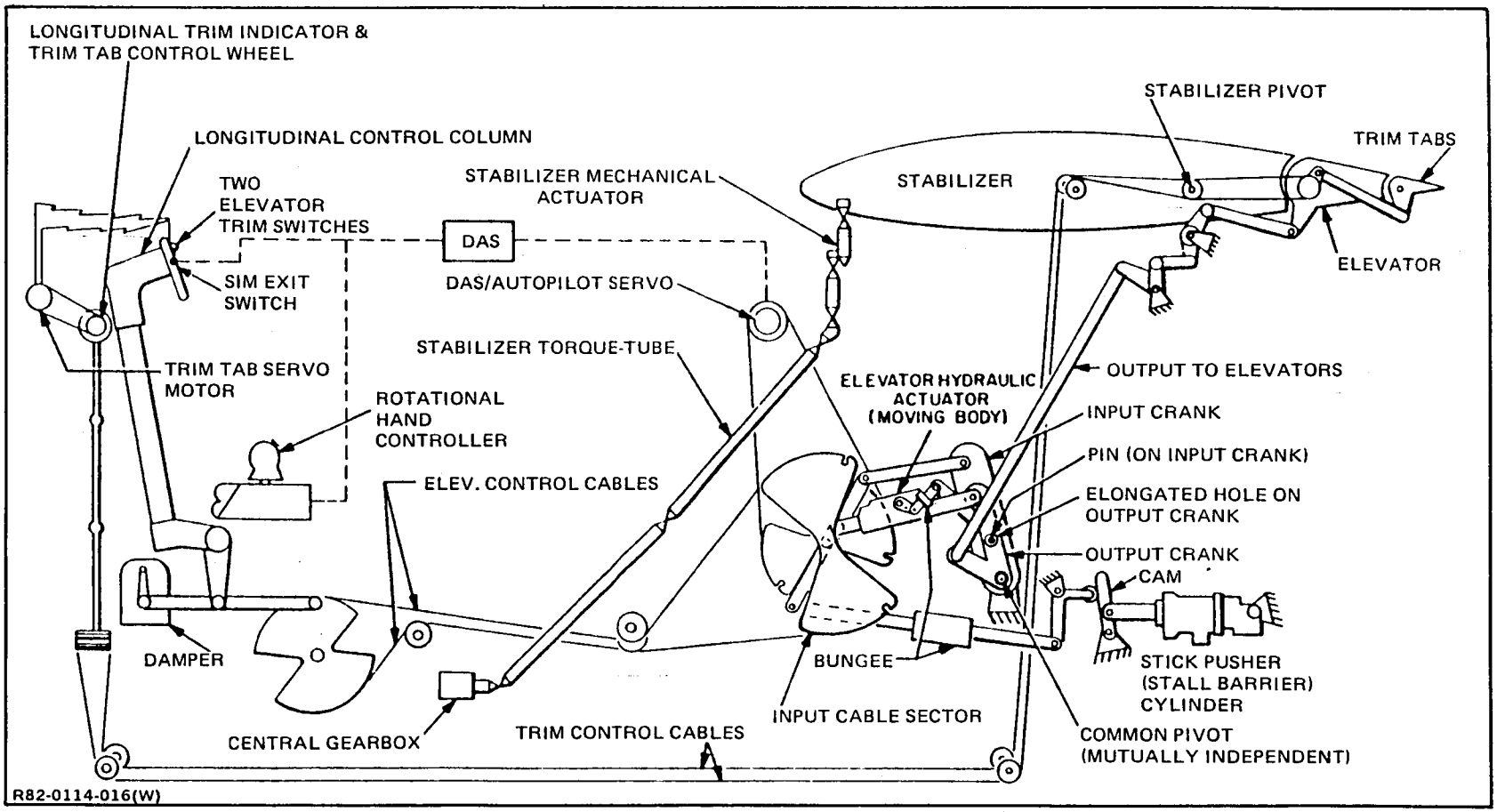


Figure 107 STA Longitudinal Control System - Schematic

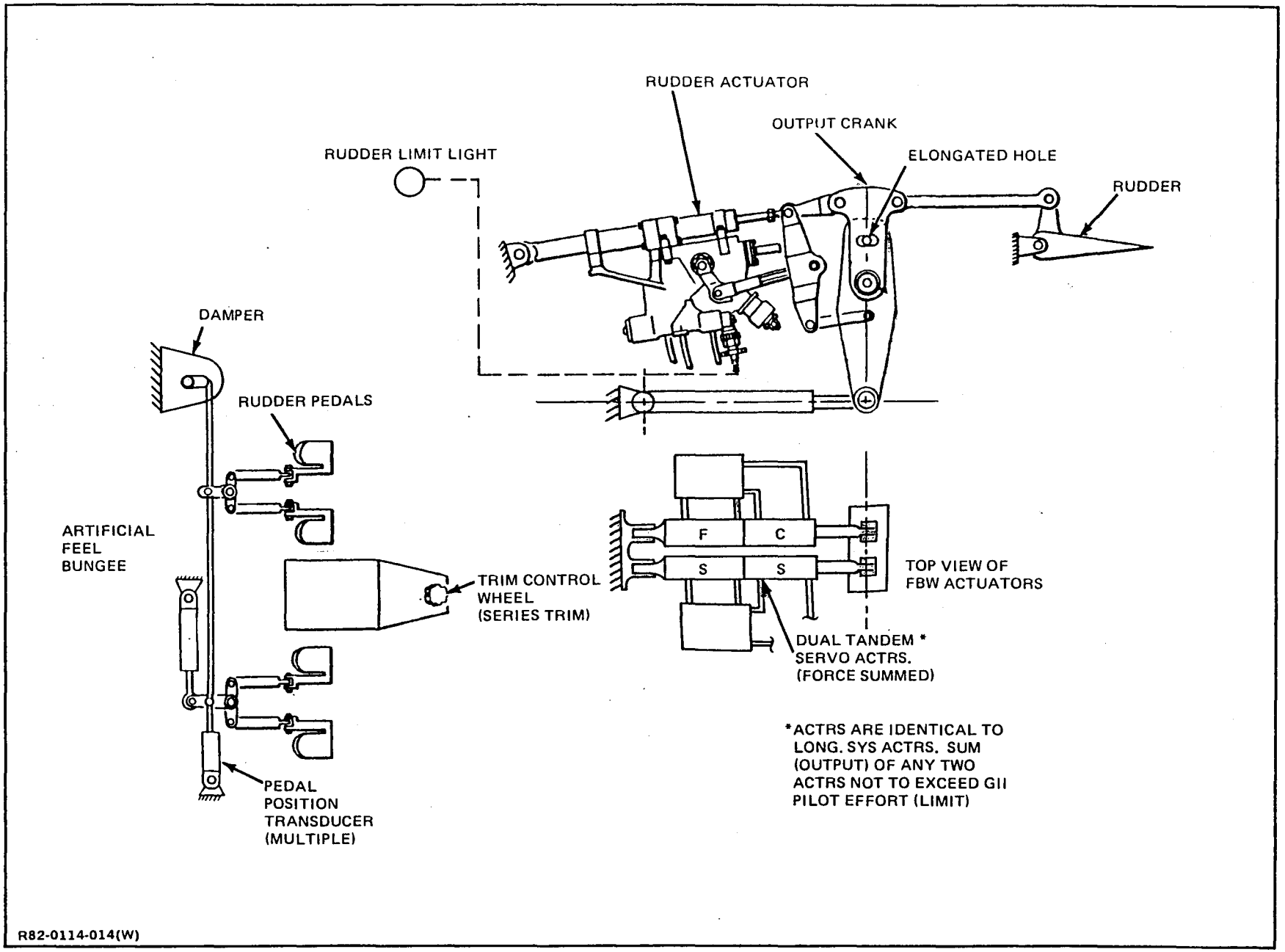


Figure 108 FBW Gulfstream Longitudinal Control System Schematic

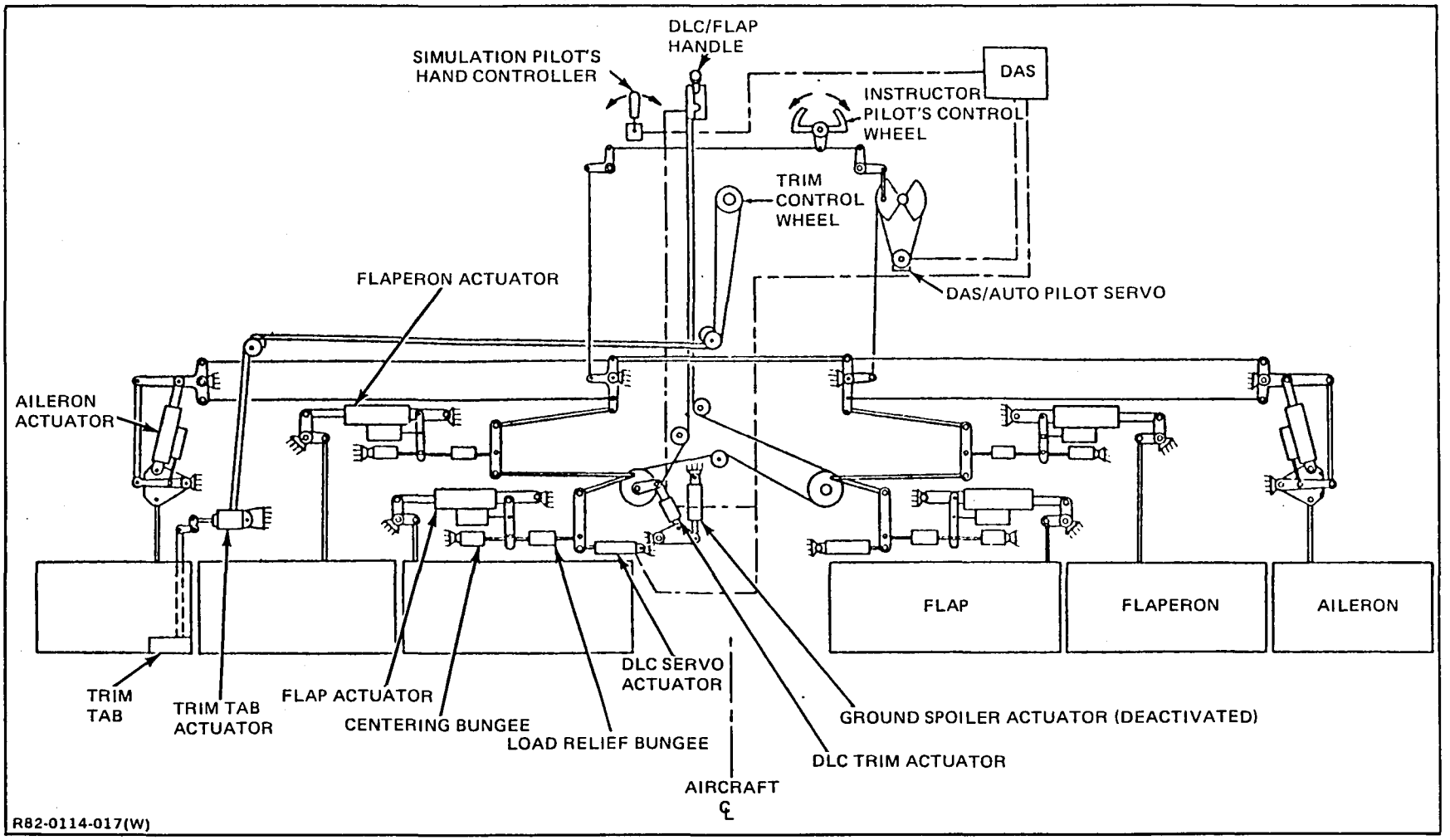


Figure 109 STA Lateral Control System - Schematic

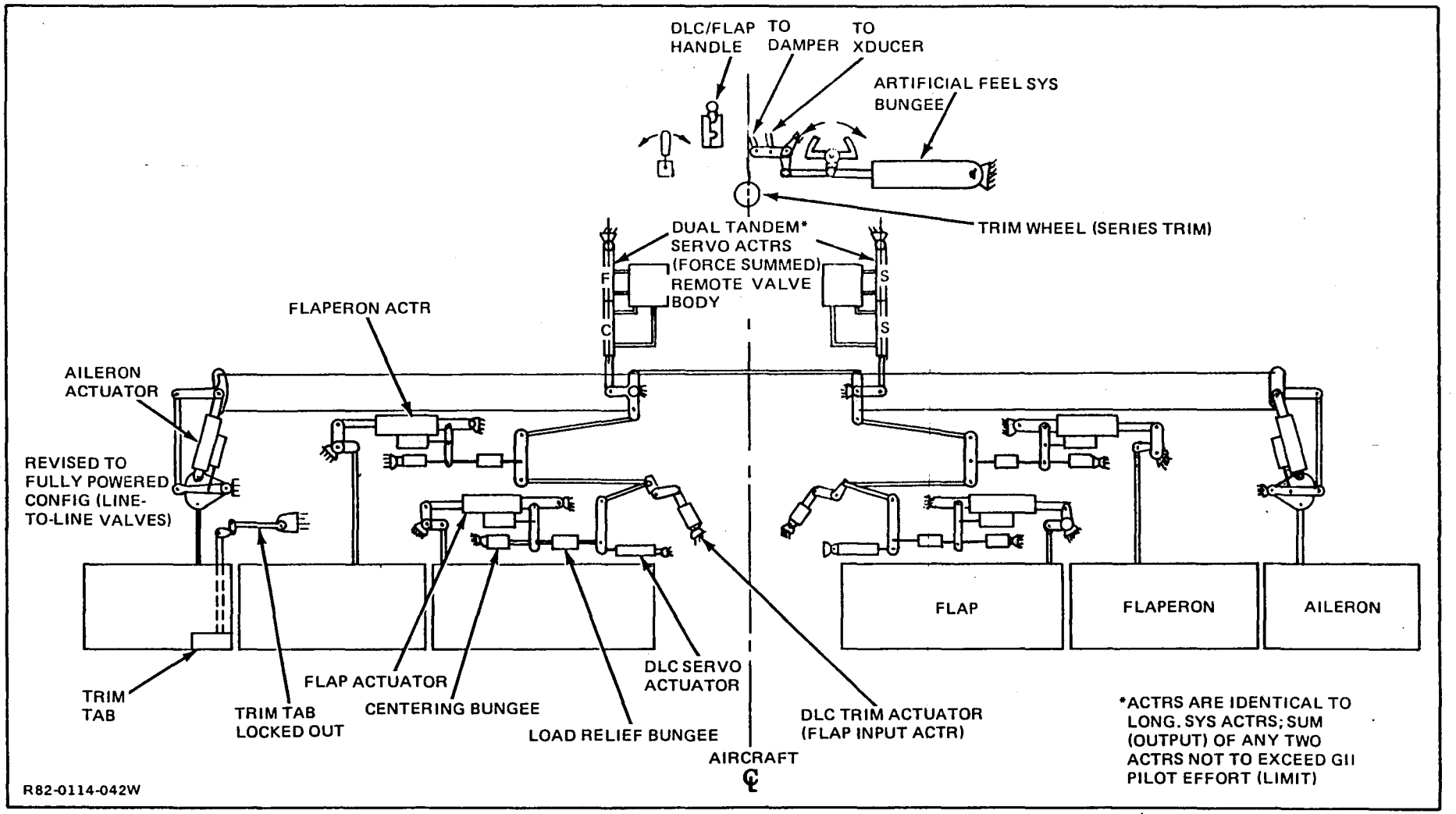


Figure 110 Lateral Control System Schematic, FBW Gulfstream

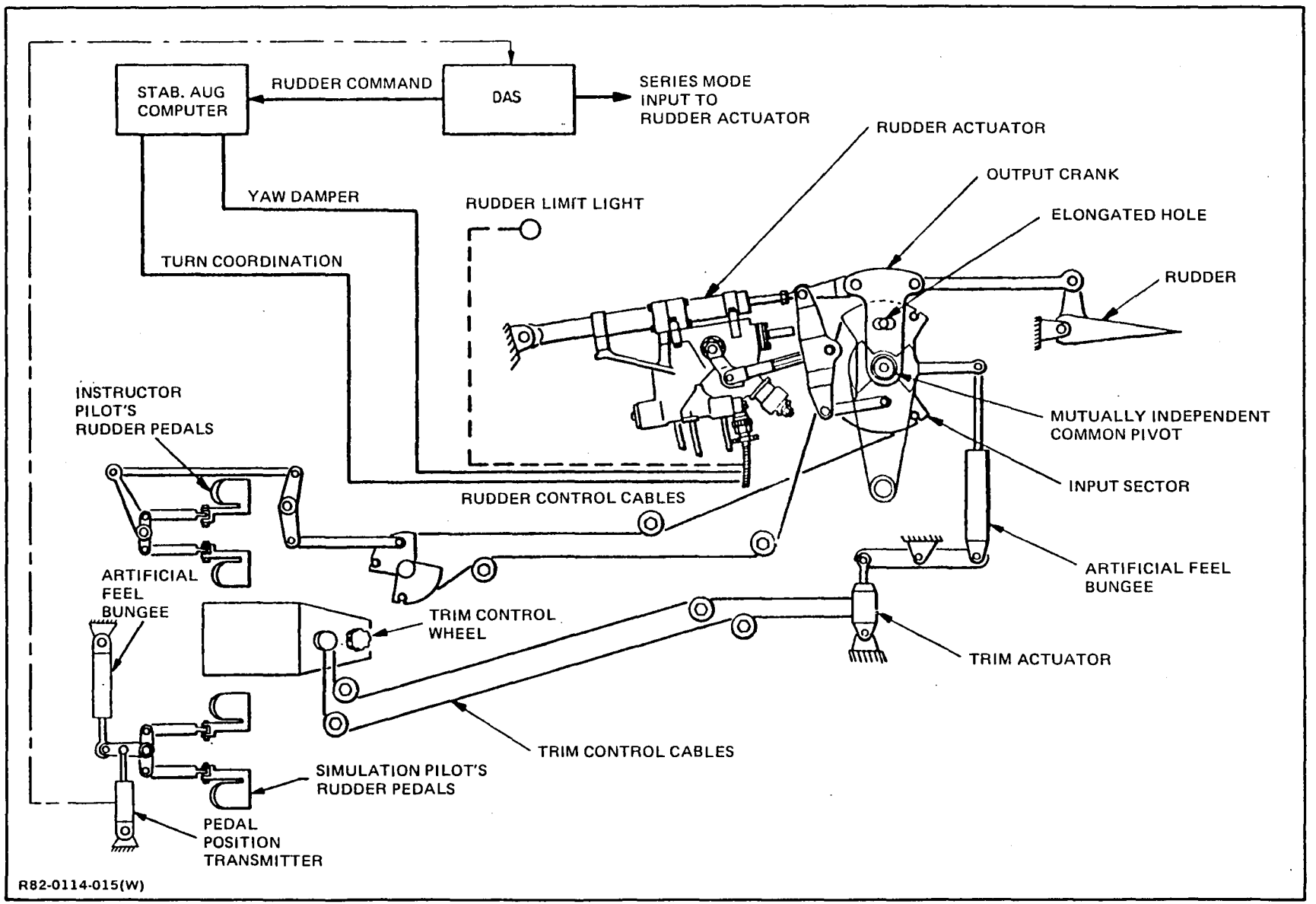


Figure 111 STA Directional Control System Schematic

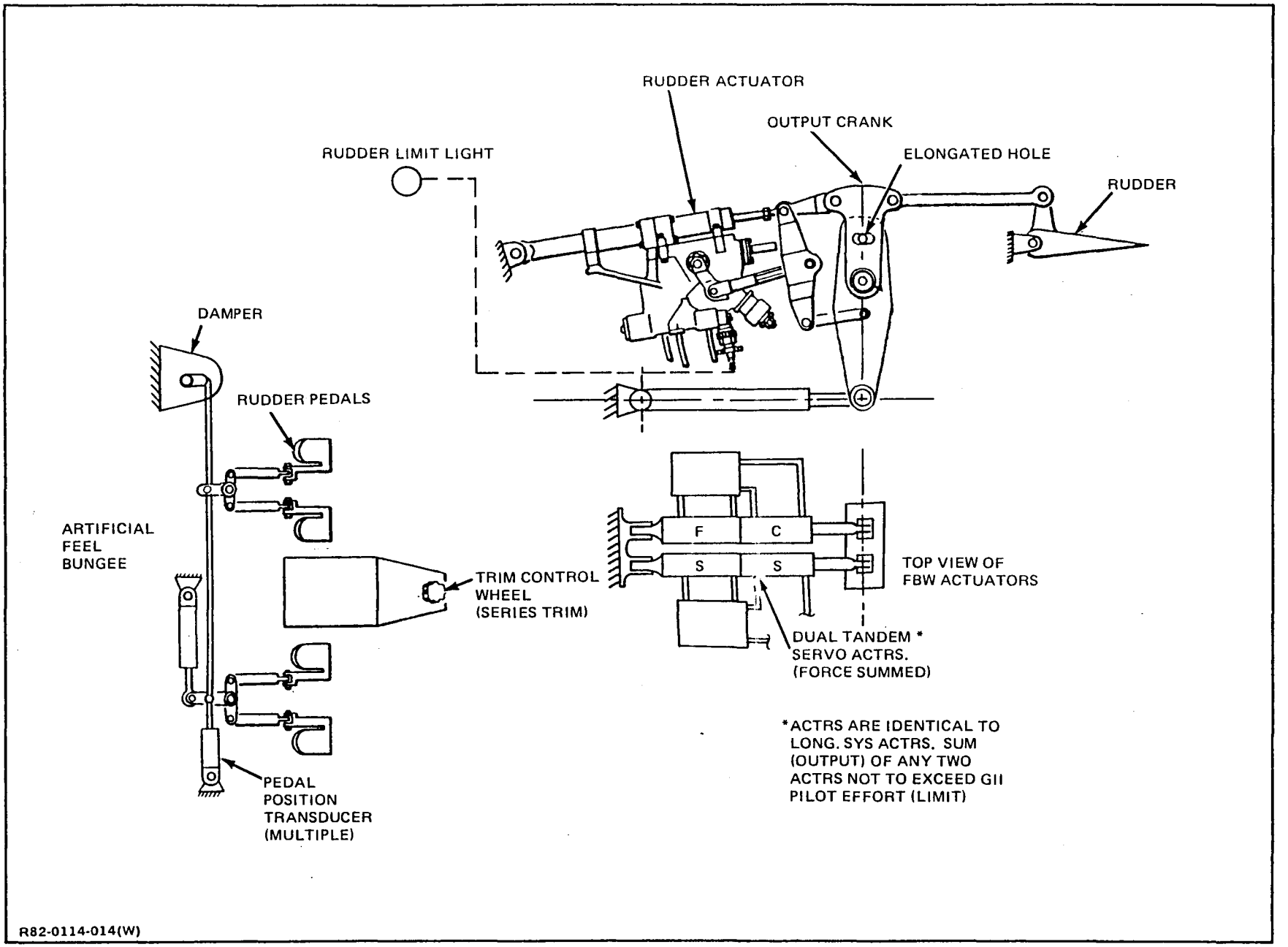


Figure 112 FBW Gulfstream Directional Control System Schematic

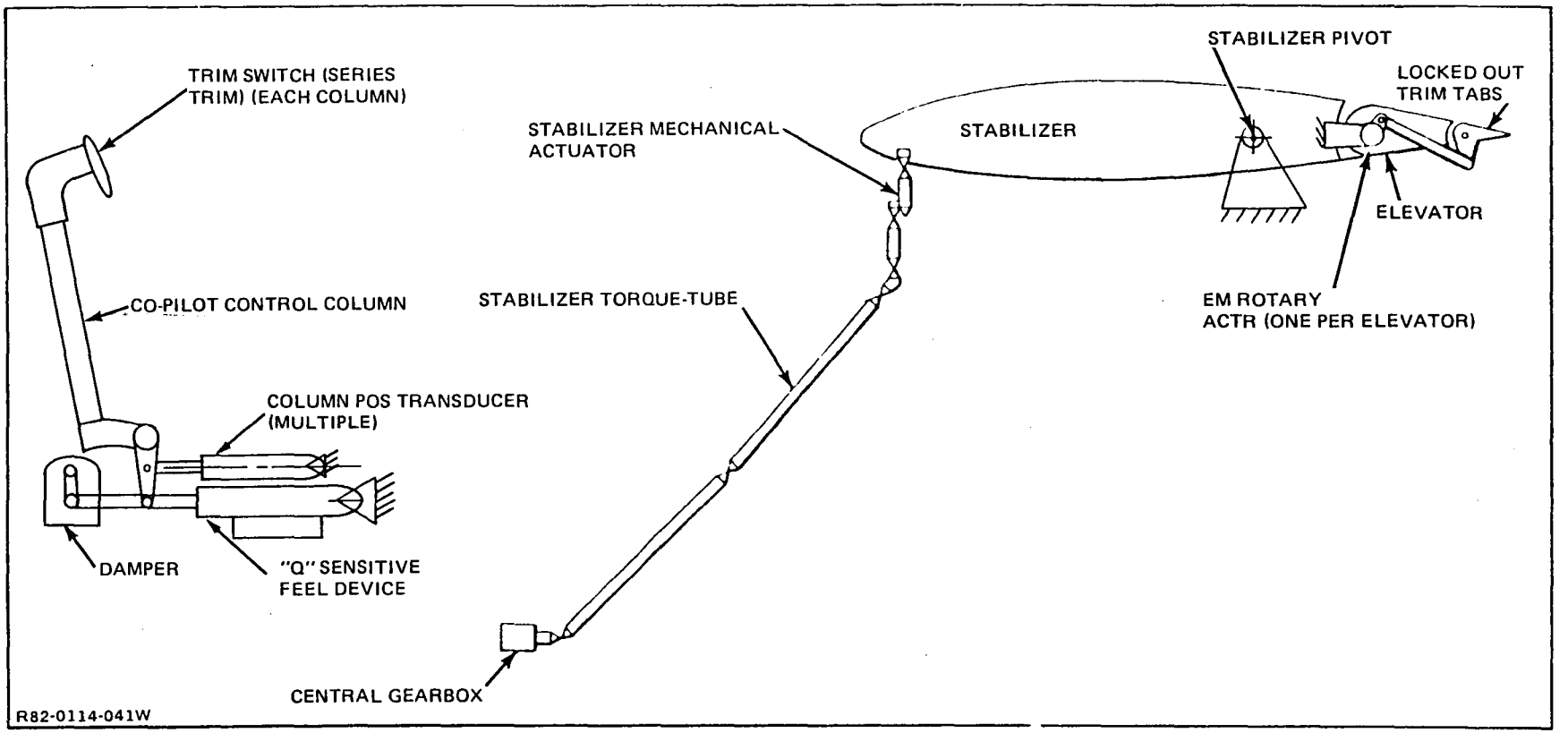


Figure 113 **Longitudinal Control System Schematic, All Electric FBW Gulfstream**

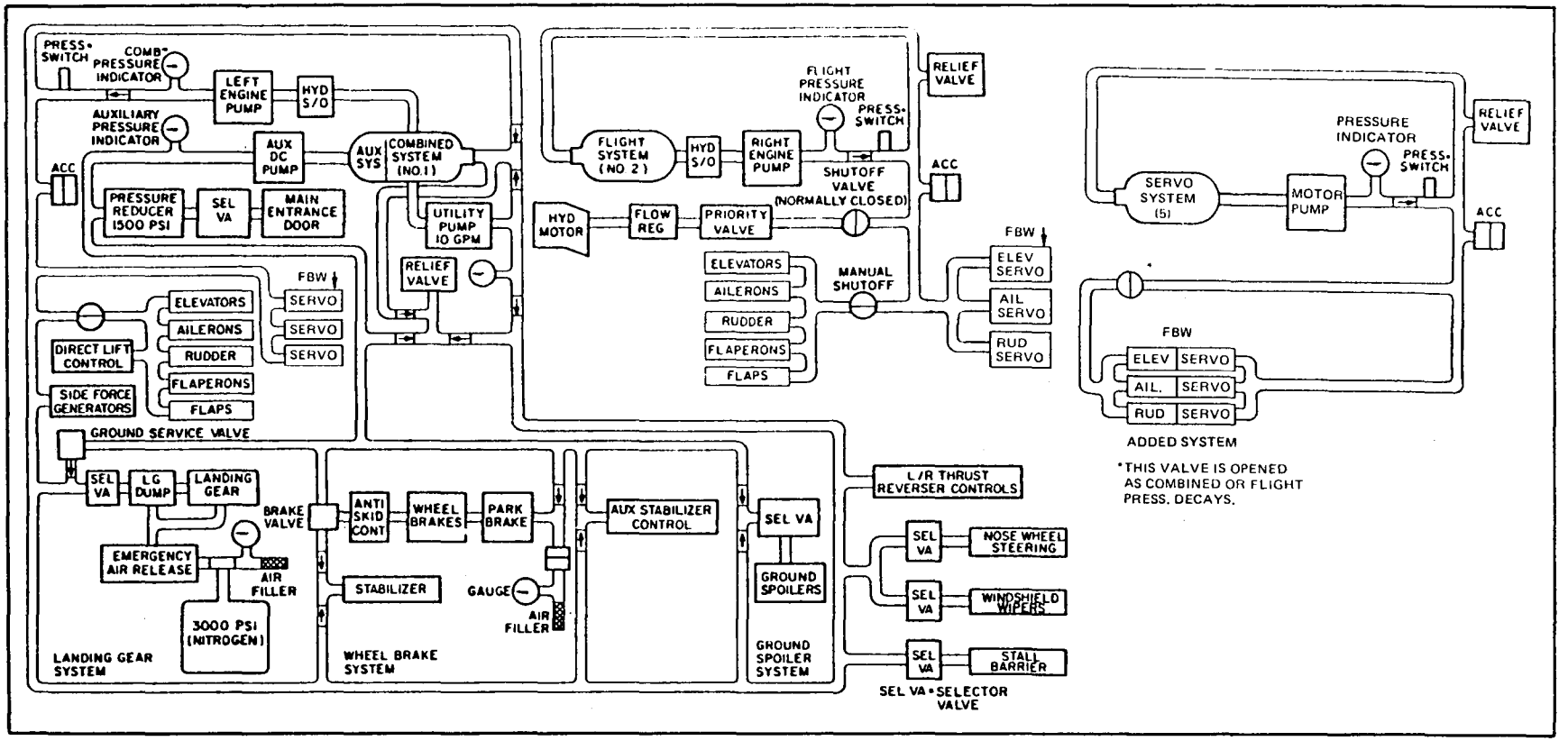


Figure 114 Hydraulics Block Diagram - FBW Gulfstream

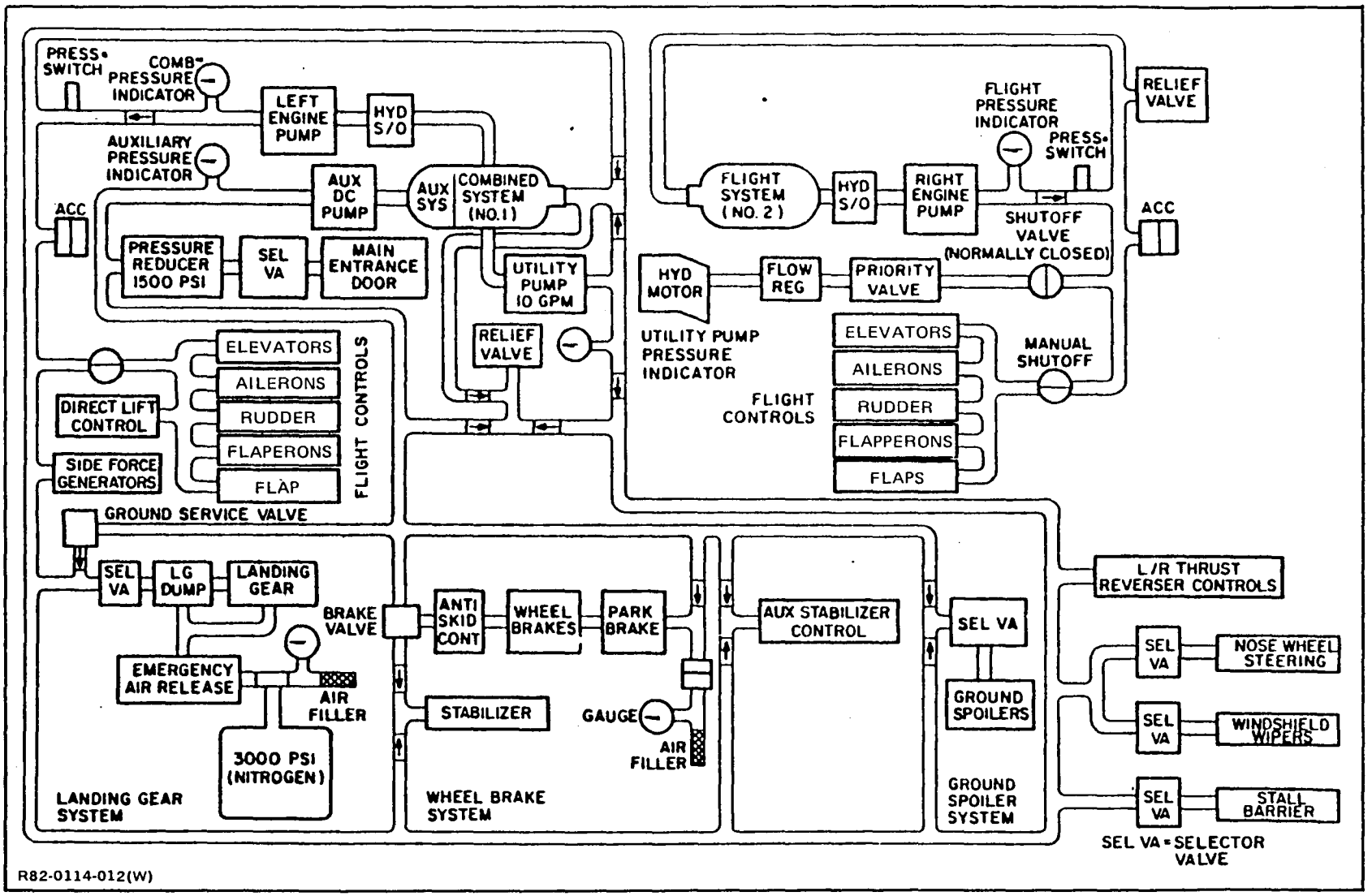


Figure 115 STA General Hydraulics Block Diagram

APPENDIX J

STA ELECTRIC POWER SYSTEM MODIFIED FOR DFBW

1. System Description

The Electrical Power System has a number of changes necessary to upgrade to Digital Fly-By-Wire (DFBW) capability. Most important of these is the requirement to make DFBW power uninterruptible; i.e., "glitch"-free. Since current power quality specifications (essentially MIL-STD-704) permit both DC and AC voltages to go to zero for up to 7 seconds during either bus switching or fault clearing operations, and DFBW equipment cannot have input voltage dip below 18 VDC (for 28 VDC) nominal input under any circumstances, additional power equipment and changes in power interface design are needed. Another important consideration is that DFBW is a flight-safety critical system; thus, reliable power must be maintained throughout the flight from takeoff through landing. In particular, the emergency sources (main batteries) must have their reliability upgraded from the present design. In brief, the changes proposed are:

- Increase battery size from 34/36Ah each to 50/60Ah each to allow for a 30-minute fail-safe period (last failure to safe landing). Replace battery monitor/bus float charge design with battery charges, and impose stricter maintenance requirements.

- Utilize remotely operable circuit breakers for DFBW in-line functions, and main source control to provide the following:

  - Automatic switchover to back-up sources/busses
  - Multi-mode fault protection (overload, over-under-voltage, underfrequency, etc.)
  - Power/load management to assure sufficient power/energy for DFBW and other flight-safety-critical systems.

- Couple each source to each DFBW channel power interface individually via circuit breaker and diode.

- Configure each DFBW channel power interface to include transient suppression and filters.

- Flight rate two (2) 20KVA or more (1) 40KVA APU to 29000ft. (new maximum operating altitude).

- Eliminate 800 Hz DAS inverter.

The balance of the equipment complement, and most of the power system monitoring will remain the same as the present configuration.

2. Change Comments

With a full-rated APU running all the time, DFBW power will be dual fail-op, but the rest of the aircraft may not be. If both DC generators have failed, an attempt to maintain cruise causes the total AC load to be $\sim$ 27KVA, meaning that at least two alternators must be on line. If the DC generator failures are both due to a power take-off problem, this causes loss of both wild frequency alternators as well, leaving only one alternator on line (APU). As a baseline, then, it will be assumed that only DFBW power will be dual fail-op, so that loss of both DC generators does abort the STA mission, but still leaves DFBW fully capable. (It should be noted that loss of both DC generators is a worse case than loss of one DC and one wild frequency alternator.)

Table 18 is a first estimate of critical load totals for three conditions:

- Cruise during training mission

- Landing during training mission

- Emergency, mission aborted.

The cruise and landing conditions were chosen to give a feel for relatively normal training flight. The figures were modified from a baseline STA by eliminating DAS and substituting DFBW. The only significant effect was addition of about 33 Amps DC. The extra current represents enough additional battery capacity for emergency conditions that an increse in size from 34/36 Ah to 50/60 Ah became necessary to continue to allow a full 30-minutes to safe landing.

Because the main batteries must be available for flight-safety-critical equipment (DFBW), the reliability penalties associated with bus-float charging can no longer be tolerated. Better chargers are therefore introduced. These add about 1.75KVA to the alternator load--an insignificant amount. The batteries will also be subject to stricter requirements for maintenance in terms of frequency, cell balance, reconditioning and electrolyte/water tests. Cell balance requirements for new battery purchase will be more stringent as well.

The primary purpose of using circuit breakers in the source-DFBW interface coupling is protection of the sources from feeder and/or channel failure. The coupling diodes act as a power OR gate, so that only the highest voltage source delivers power, and all other diodes are back-biased. It can be seen from this that, with all sources available, all circuit breakers are normally closed to permit the smoothest transition from one to another. If a source fails, the circuit breaker associated with its feeders to each interface will be tripped by command following transition to a back-up.

The "glitch" suppression batteries are tentatively sized as 3 Ah ("D" cell) sealed nickel-cadmium in a 20-cell configuration. Each string will be diode coupled to a DFBW channel power interface; so will be open-circuited when not needed. Actual steady-state minimum voltage at the power interface will by 20 x 1.0-0.8=19.2V, comfortably above the required 18V level. However, during each transition, the battery has a rise time of $\sim$ 1-5 microseconds. To maintain interface voltage in this period, a small capacitor will be used. Overvoltage spikes and EMI will be suppressed by a combination of absorption and filtering devices. The "glitch" suppression batteries will not be charged on-board. At 3 Ah nominal rating, each can handle up to 15 7-second periods of zero source voltage, or retain up to 4 such events for 10 days without maintenance. It is desirable, then, to remove the strings after either 10 days or 10 events (whichever is first) for reconditioning and test. The same restrictions on cell balance obtain for these as for the main batteries. In order to assure that a string is healthy while on the aircraft, each will be monitored by a tapped sensor which can detect a 1-cell failure or degradation by determining the difference in voltage between the two halves of the string. The sensor is designed to draw current at least two orders of magnitude below self-discharge equivalent ($\sim$ 5.25 mA maximum for this size cell).

Additional weight due to new components and upgraded ones are estimated to be as follows:

- Battery chargers $\sim$ 30 lb.
- "Glitch" suppression equipment $\sim$ 50 lb.
- Main battery increase $\sim$ 100 lb.
- Diodes, breakers, feeders, etc. $\sim$ 25 lb.

These figures do not account for reductions due to removal of DAS equipment, nor additions ude to structure. It seems certain the battery compartment will require major modification, and that the power distribution system and cockpit control panels will too.

Figure 116 shows in block form, the basic DC system of the present STA. It was taken from the STA Maintenance Manual. Sketched on the figure is the Area of Change to modify the system for DFBW. Figure 117 is that Area of Change so modified. Figure 117 shows an n-channel DFBW, but the load and weight estimates above are for a 4-channel system.

3. Auxiliary Power Unit

The Gulfstream II STA auxiliary power unit (APU) provides hot compressed air for ground air conditioning and engine starting. A 20K VA alternator mounted on the APU accessory case provides electrical power for use when neither of the engine-driven generators is operating. Controls and indicators for the APU are located on the center overhead panel. The APU is installed in the tail compartment aft of the pressure dome, and is equipped with its own fire detection and extinguishing systems.

The APU is self-regulating, essentially requiring only start and stop commands from the cockpit. Self-contained control devices continue the start sequence after it is initiated at the center overhead panel, maintain constant speed under varying load conditions, and automatically perform a shutdown sequence if certain temperature, pressure, or overspeed parameters are exceeded.

The APU is currently limited to ground operation. Power connections through the nutcracker system prevent starter operation if the aircraft is airborne, and APU shutdown is automatic if the aircraft becomes airborne with the APU operating. The APU installation in the Gulfstream I is flight rated.

The APU is flight rated for the envelope shown in Figure 118. A brief outline of the steps for flight rating the APU as installed in the FBW Gulfstream follows:

1. Change mount structure to steel

2. Modify or change flex ducts to improve fire proof capability

3. Add heat shield to aircraft skin

4. Modify controls for in flight starting

   No nutcracker interlock
   Add bleed surge dump

5. Modify bleed surge dump ducting
6. Add interlocks to prevent unit bleed when main engine air is used
7. Modify fuel control to fine speed control if frequency is critical
8. Flight test compartment cooling scheme
9. *Flight test starting and operating capability
10. Modify fire detection system to permit inflight checking
11. Fireproof inlet duct to skin
12. Add second fire extinguishing system.

*Should be capable of 20,000 ft. starts and 30,000 ft. operation.

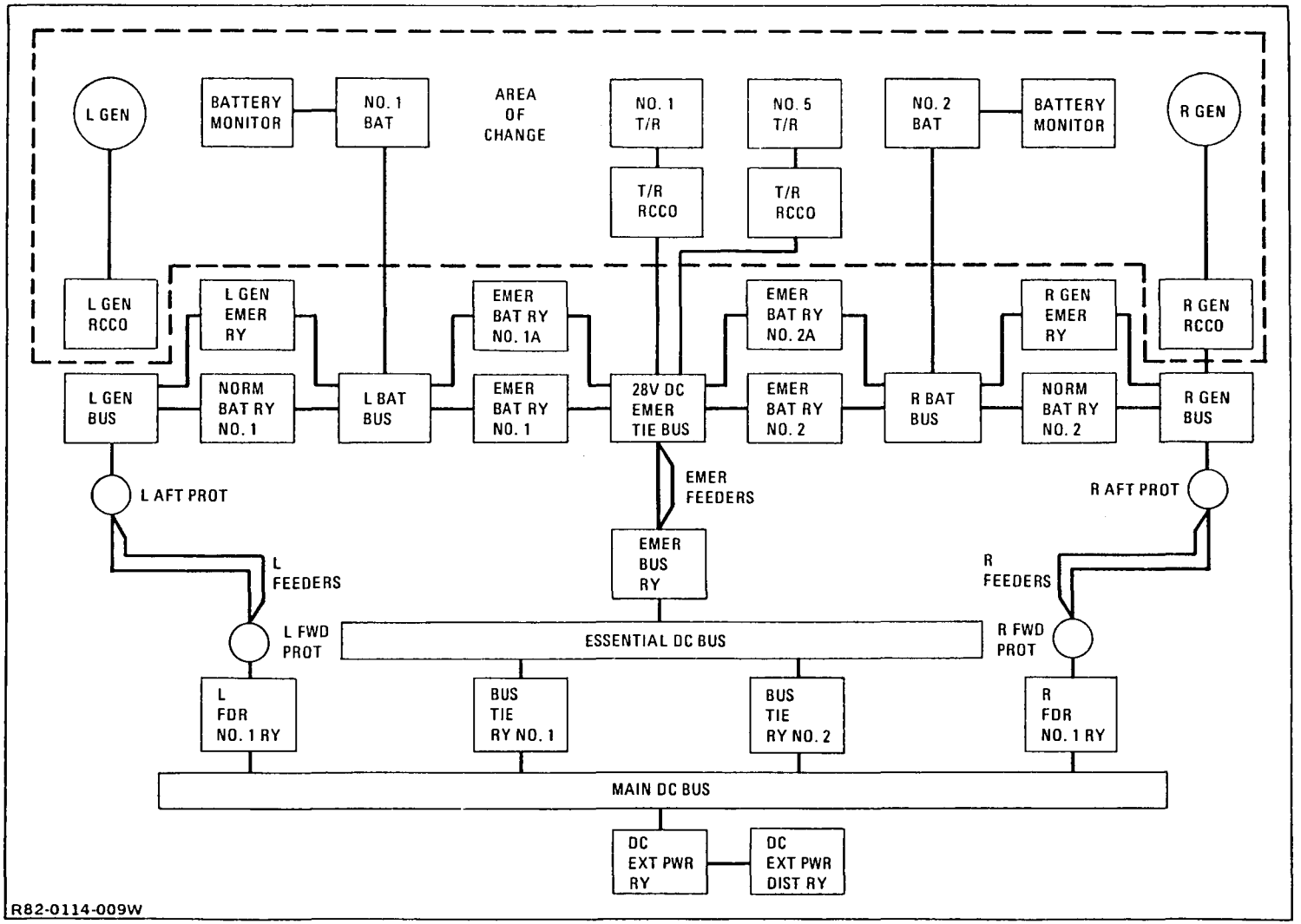


Figure 116 Basic STA-FBW DC System

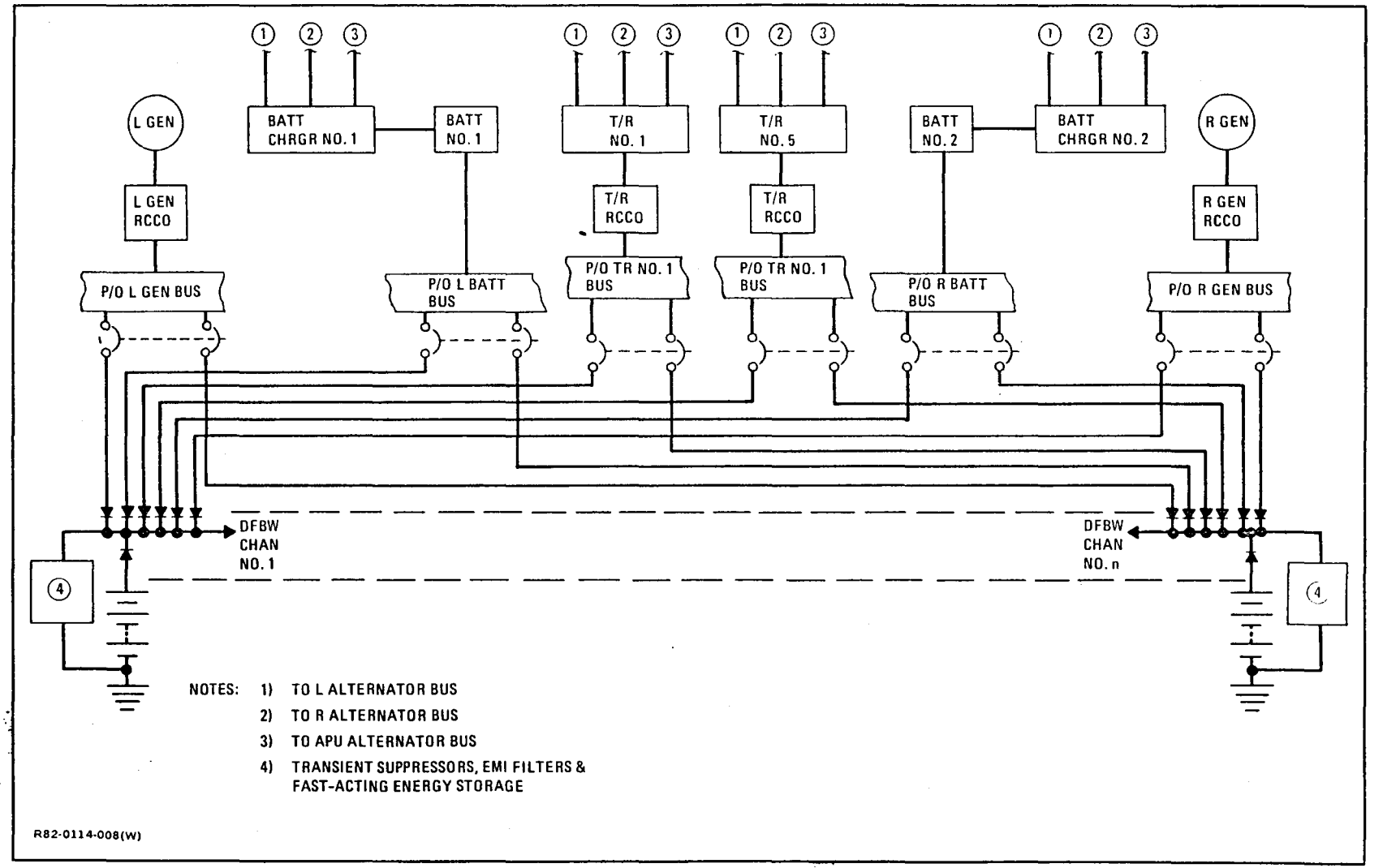


Figure 117 Changes to Basic STA DC System for FBW Gulfstream

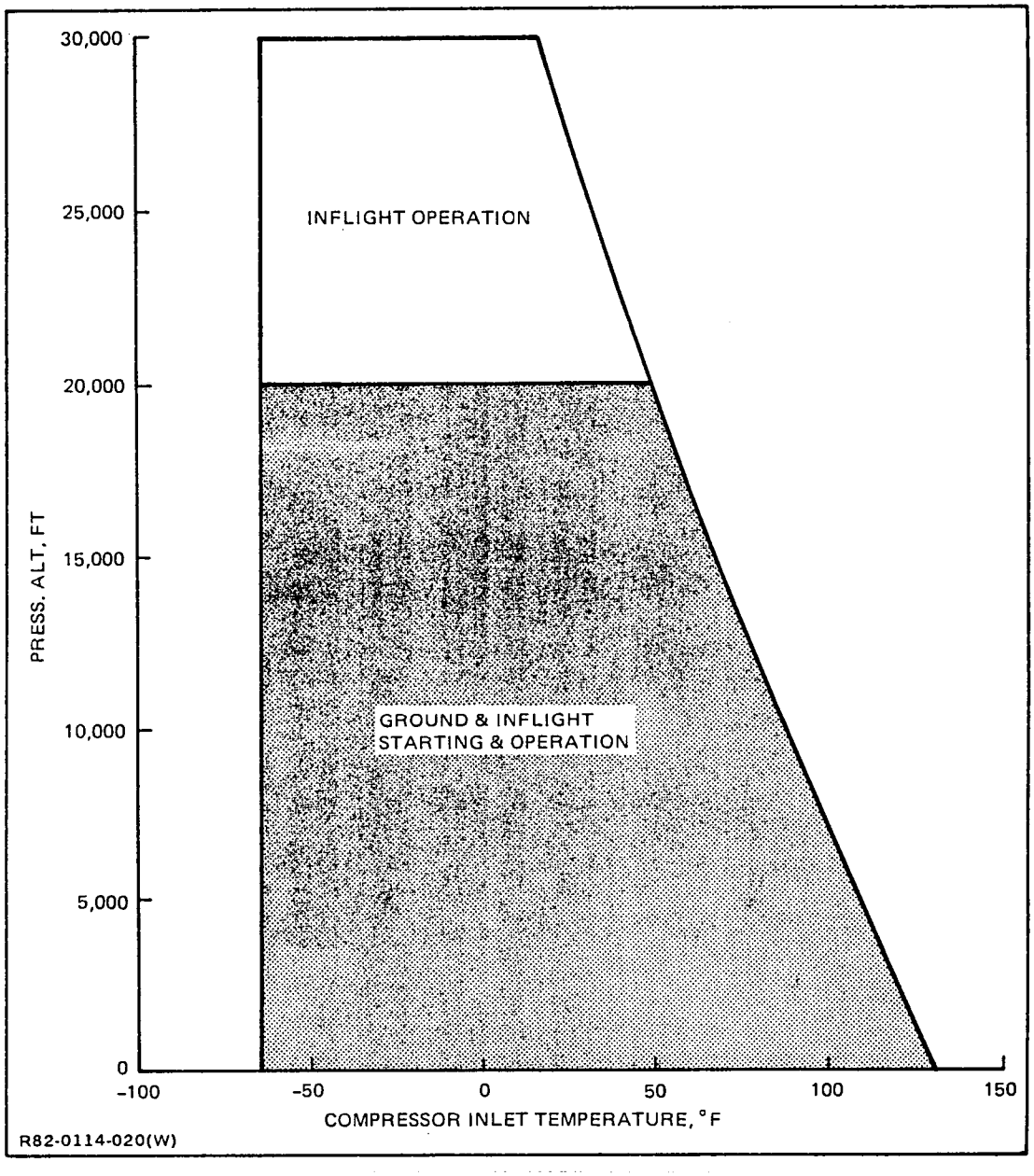


Figure 118 **Starting & Operating Envelope for Model GTCP36-100, Auxiliary Power Unit**

Table 18 Critical Loads Estimate - STA vs. FBW Gulfstream

SOURCE	STA								FBW GULFSTREAM							
	RATING	OVER-LOAD RATING	LOADS						RATING	OVER-LOAD RATING	LOADS					
			CRUISE		LANDING		EMERG*				CRUISE		LANDING		EMERG*	
			VALUE	%	VALUE	%	VALUE	%			VALUE	%	VALUE	%	VALUE	%
DC GENERATORS	300A	450A	241.3A	80.4	399.8A	133.3	123.6A	41.2	300A	450A	274.4A	91.5	432.9A	144.3	156.7A	52.2
ALTERNATORS	20.0 KVA	N/A	14.9 KVA	74.5	14.9 KVA	74.5	14.5 KVA	72.5	** 20.0 KVA	N/A	16.7 KVA	83.5	16.7 KVA	83.5	14.5 KVA	72.5
BATTERIES-MAIN	2 PAR 34/36 AH EA.	N/A	–	–	*** –	–	61.8 AH	88.3	2 PAR 50/60 AH EA.	N/A	–	–	*** –	–	78.4 AH	71.3

* ASSUMES ONE OR BOTH DC GENERATORS & BOTH MAIN ALTERNATORS ARE OUT. 30 MIN ALLOWED FOR SAFE LANDING

** SECOND FULL-SIZE APU REQUIRED FOR HYDRAULICS (OR SINGLE 40 KVA). APU FLIGHT RATED TO STA CEILING OF 30K FT, & IS OPERATED THROUGHOUT FLIGHT

*** BATTERIES MAY SUPPORT THIS CONDITION IF COMBINATION OF DC GENERATORS & T-Rs IS INSUFFICIENT

R82-0114-010(W)

APPENDIX K

SHUTTLE TRAINING AIRCRAFT GUIDANCE, NAVIGATION, AND CONTROL SYSTEMS

The guidance, navigation and control system provides the STA Digital Avionics System (DAS) with attitude, velocity, acceleration, and position data for computation of flight parameters and control commands. The equipment comprising the guidance, navigation, and control systems is listed in Table 19.

Functional Description (See Figure 119)

The following paragraphs describe the relationship between the navigation and guidance system inputs and the Digital Avionics System (DAS).

A. Rotational Hand Controller

The rotational hand controller is used by the Simulation Pilot to apply pitch and roll rate commands to the DAS in response to aircraft attitude change requirements when the aircraft is being operated in the manual simulation mode. The pitch and roll rate commands are proportional to the displacement of the rotational hand controller. When the rotational hand controller is returned to its spring-loaded center detent position in either roll or pitch, zero attitude rate is commanded and the existing attitude is maintained. The rotational hand controller also provides orbiter pitch and roll trim commands and a takeover discrete to allow the Instructor Pilot to take over control of the aircraft and operate it in the manual mode.

B. Microwave Scan Beam Landing System

The Microwave Scan Beam Landing System (MSBLS) provides the DAS with azimuth, elevation, and range to touchdown during simulated final approach and landing when operating the aircraft in the simulation mode. All data is transferred to the DAS on a serial data line.

C. TACAN

The TACAN provides the DAS with range and bearing data, referenced to a ground based TACAN station. This data is used by the DAS in the simulation mode during the energy management phase to compute position and bearing relative to the heading alignment circle, and during the approach and landing phase to compute range and bearing to the runway threshold.

D. Inertial Navigation System

The Inertial Navigation System (INS) provides the DAS with pitch and roll attitude data in synchro format and vertical acceleration in analog format. The INS also provides the following data in binary format to the DAS on a serial digital data line: latitude, longitude, true heading, wind speed, wind angle, north-south velocity, east-west velocity, cross track deviation, track angle error, and drift angle. Two valid output signals are also provided; one for pitch and roll signals and one for the binary data.

E. VHF Navigation System

The VHF navigation system provides the DAS with VOR bearing information for radio navigation and glidescope/localizer deviations for display and guidance during approach and landing with the aircraft operating in the manual ILS approach and the autopilot mode. The information is displayed on the Instructor Pilot's horizontal situation indicator and attitude indicator. Three valid output signals are provided: localizer; tune-to-localizer; and glide slope.

F. Gyrocompass System

The gyrocompass system provides gyro stabilized magnetic heading information for display on the system radio magnetic indicator (RMI) and for use by the digital avionics system (DAS), VOR/ILS systems, TACAN system, heading situation indicator (HSI), and the flight recorder. Two independent gyrocompasses are provided. Gyrocompass No. 1 is the primary gyrocompass for the Instructor Pilot and No. 2 is primary for the Simulation Pilot. However, either gyrocompass can be selected for operation by either pilot by selecting COMP 1 or COMP 2 with INST SWITCHING controls on the center pedestal and the Instructor Pilot's flight panel. The gyrocompass is a standard gyro-stabilized compass. Aircraft

magnetic heading is sensed by the flux valve and transmitted to the RMI via the remote magnetic compensator. The RMI displays the magnetic heading and also provides heading information to the compass switching circuits for distribution to other navigation systems and flight recorder. Gyrocompass No. 2 RMI also displays TACAN bearing on both pointers simultaneously.

G. Radar Altimeter System

The radar altimeter system provides the Instructor Pilot with an accurate indication of the aircraft's altitude above the terrain for altitudes up to 5,000 feet. The system also provides the digital avionics system (DAS) with altitude data for computing final flare altitude during final approach. The radar altimeter system equipment are all components of Electronic Altimeter Set AN/APN-194(V).

H. Central Air Data Computer

The central air data computer provides the DAS with altitude, airspeed, and Mach number data as shown in Figure 119. The central air data computer also provides the altitude, airspeed, and Mach number signals to the Mach airspeed and servo altimeter systems for display on the cockpit instruments. True airspeed data is also provided to the INS. Temperature reference is provided to the central air data computer by the total temperature sensor. Four valid output signals are provided; altitude; computed airspeed (CAS); Mach number; and true airspeed (TAS).

I. Autothrottle Servo System

The autothrottle servo system provides automatic computer control of engine power during simulation mode operation. A servo interlock control unit in the Digital Avionics System (DAS) contains the servo control loops and interlock electronics that drive the autothrottle servo in response to commands from the DAS computer. The autothrottle servo is mechanically linked to the throttle levers and controls engine power through the same linkage as the throttle levers. Engine power is varied to allow the aircraft to simulate the orbiter airspeed and attitude characteristics. The throttle settings are determined by the DAS computer using inputs from the aircraft instrument and navigation systems for comparison with orbiter requirements. The computer then generates either increase or decrease throttle drive signals.

J. Data Acquisition

The purpose of data acquisition system is to record a set of preselected parameters. All data recording is controlled by the Digital Avionics System. The start and stop modes are keyboard controlled. START mode implements recording, and is initiated any time the DAS system is powered up; recording can be eliminated by use of the STOP mode. Both modes are overridden by the AUTO mode which initiates recording whenever SIM is engaged.

The automatic recording mode, which is activated during SIM engage, is implemented with an automatic timed-out stop after SIM disengage. The timed-out clock can be loaded with any value between zero and 120 seconds by the GNS routine. If an earlier stop than the value of the clock is anticipated, termination of recording can also be accomplished by entering the stop mode via the REC mode. This premature stop provision of the automatic mode is available only during the time-out phase. The data recording routine automatically checks status of the magnetic tape unit. Once this occurs, recording will start with 273 words being recorded every 50 millisecond cycle.

During the record mode, an interrupt is received from the magnetic tape controller after the completion of each recorded record. Status is then checked to determine if a valid condition still exists. Five different forms or packages of the data are transmitted to the data acquisition system:

- A/D inputs (12 bits) +6 bit discretes
- D/A outputs (12 bits) +6 bit discretes
- Serial input words (36 bits)
- Serial output words (36 bits)
- Miscellaneous orbiter model and STA parameters

Negative logic is employed; zero states are true, and ones are false. All input and output words are recorded from their respective raw data buffers. Miscellaneous parameters are first buffered before a record transfer is initiated.

Decoding synchro inputs and cancelling reference voltage fluctuations and gains introduced in the A/D converter are performed.

K. Air Data Systems

The Pitot and Static Pressure Systems supply impact (Pitot) and atmospheric (Static) pressure to various instruments and equipment.

The Pitot System obtains its pressure from the Pitot Probes located on the left and right side of the fuselage at station 63. The Left Pitot Probe supplies impact pressure to the ARINC 565 Air Data Computer and Flight Recorder. The Right Pitot probe supplies impact pressure to the Instructor Pilot's Mach Airspeed indicator, Overspeed Warning Sensor and 844 air Data Computer.

The Static System obtains its pressure from Flush Static Vent Systems No. 1 and 2. These two vents are located on the sides of the fuselage at station 196. From the Static Vent System No. 1, static air is piped to the Alternate Static Selector Valve System No. 1, where the static air is forwarded to the Altimeter, IVSI, and Mach Airspeed indicators. From the static Vent System No. 2, static air is piped to the Alternate Static Selector Valve System No. 2, where the static air is forwarded to the Cabin Altimeter, Differential Pressure gage, Overspeed Warning Sensor, 844 Air Data Computer and Flight Recorder.

If the Flush Static Vent Systems No. 1 and 2 become inoperative an alternate means of obtaining static pressure is provided. Positioning the Alternate Static Selector Valve, located on the Instructor or Simulation Pilot's Flight Instrument Panel to ALTERNATE will permit ambient air to flow through the Alternate Static Vent Systems No. 1 and 2 to supply static pressure to the equipment normally supplied by the No. 1 or 2 Flush Static Vent System. The Alternate Static Vent System also provides static pressure to the ARINC 565 Air Data Computer. There is a Pitot and a Static Shutoff Valve for the 844 Air Data Computer located on the aft end of the Instructor Pilot's Side Console. Both valves would normally be in the ON position. If a rupture in the lines should occur between the valves and the 844 Air Data Computer, the valves would be placed to the OFF position. This would retain valid Pitot and Static pressure to the Instructor Pilot's flight instruments and Overspeed Warning Sensor.

The Mach Airspeed and Servo Altimeter System monitors indicated airspeed, Mach number, and indicated altitude. The Air Data Computer provides analog and digital outputs representing pitot pressure, static pressure aircraft altitude, limited altitude correction signals, and Mach number to the indicators. All of these signals are derived from inputs into the Air Data Computer from the Pitot and Static System.

The Air Data System for FBW applications requires review as to the reliability and redundancy levels required based on the dependency of the flight control laws on air data.

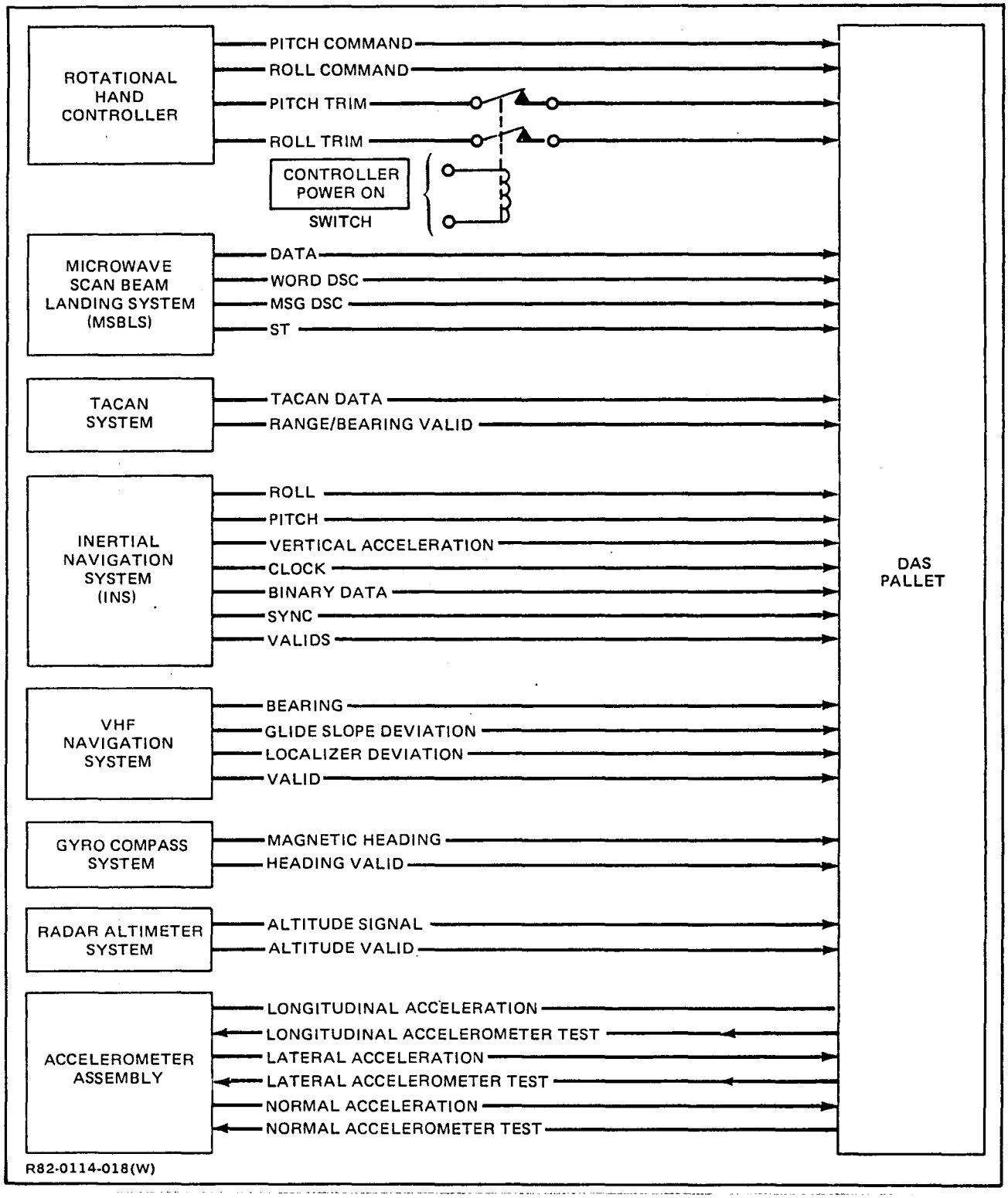


Figure 119 STA Guidance, Navigation & Control System - Simplified Block Diagram

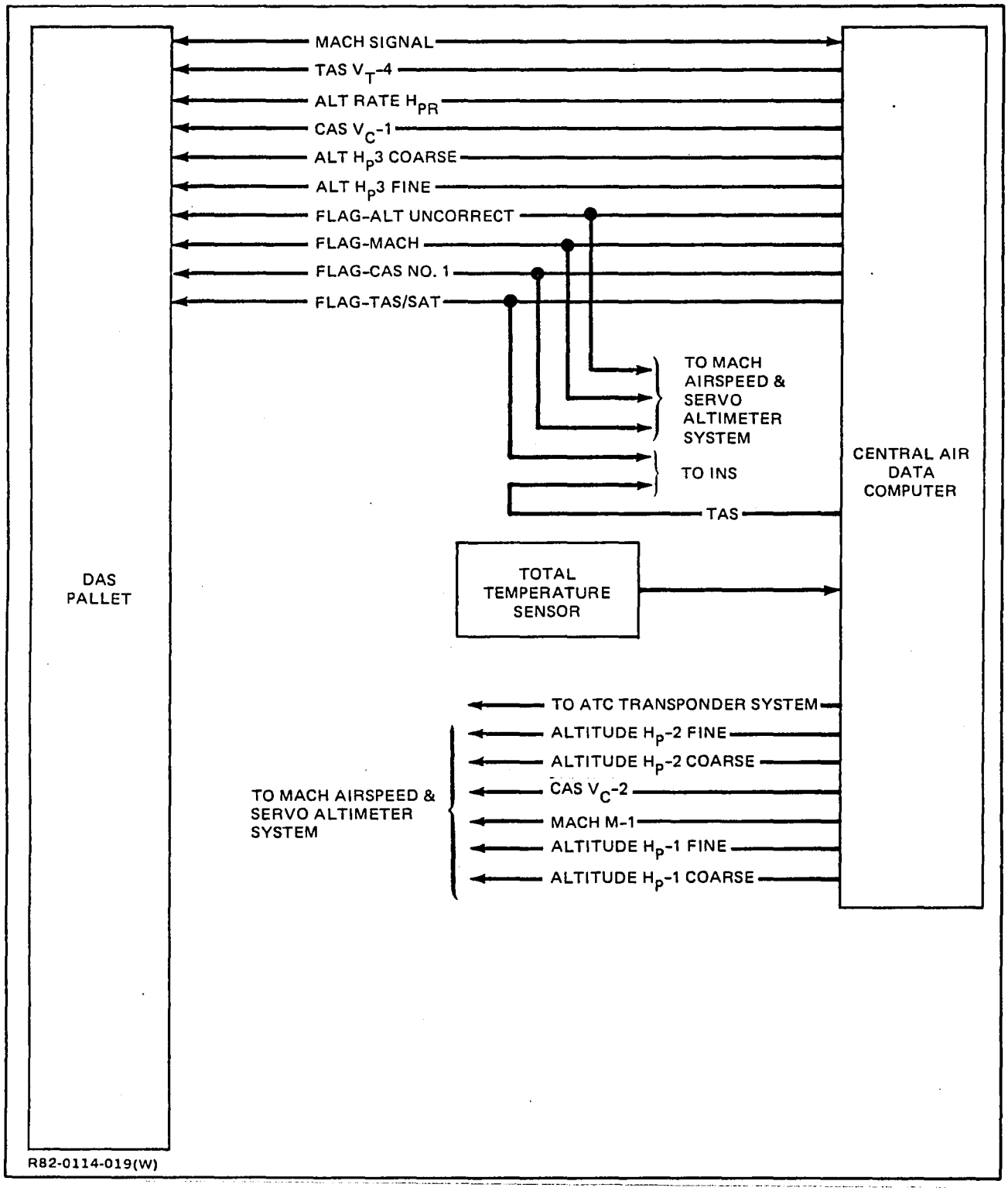


Figure 120 STA Guidance, Navigation & Control System - Simplified Block Diagram

TABLE 19

GN&C SUB-SYSTEMS

SYSTEM	TYPE
INS (Inertial Navigation System)	Litton LTN-51
Vertical Gyro (2)	Sperry VG-311
Gyro Compass System (2)	Sperry C-11B (C-6E Indicators)
TACAN	Hoffman AN/ARN-117
DME (Distance Measuring Equipment)	Collins 860E-3
Radar Altimeter	Honeywell AN/APN-194
CADC (Central Air Data Computer)	Sperry ARINC 565 Modified for 36,000 ft/min capability
VOR/ILS (2)	Collins 51RV-2B Nav Receiver
Flight Director Computers	Sperry Z-14 (SPI-77A)
DAS (Digital Avionics System)	Sperry 1819B Digital Computer
Stability Augmentation Computer	Sperry SP-50G AFCS (P/O)
Rotational Hand Controller	LM GFE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA CR- 163120		

4. Title and Subtitle	5. Report Date
Advanced Flight Control System Study	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
John G. McGough, Kurt Moses, and John F. Klafin	10. Work Unit No.

9. Performing Organization Name and Address	11. Contract or Grant No.
Bendix Corporation Flight Systems Division Teterboro, NJ 07608 Grumman Aerospace Corp. Bethpage, NY 11803	NAS 4-2877

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
National Aeronautics and Space Administration Washington, D.C. 20546	Contractor Report
	14. Sponsoring Agency Code

15. Supplementary Notes

NASA, Project Engineer: Lawrence Abbott

16. Abstract

The architecture, requirements, and system elements of an ultra-reliable, advanced flight control system are described. The basic criteria are functional reliability of 10^{-10}/hour of flight and only six month scheduled maintenance (no unscheduled maintenance). A distributed system architecture is described, including a multiplexed communication system, an ultra-reliable bus controller, the use of skewed sensor arrays, and actuator interfaces. A proposed test-bed and flight evaluation program are also discussed.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Digital flight control system, fly-by-wire, multi-processors, multi-plexed data transmission.	Unlimited

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price*
Unclassified	Unclassified	373	

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

THIS PAGE INTENTIONALLY LEFT BLANK

End of Document