NASA CR-
147657

(NASA-CR-147657) PFEVENTICN OF DESIGN FLAWS IN MULTICCMPUTER SYSTEMS (McDonnell-Dcuglas Technical Services) 114 p HC $5.50 CSCL 09B

N76-23889

Unclas

G3/61 41452

PREVENTION OF DESIGN FLAWS

IN

MULTICOMPUTER SYSTEMS

DN 1.3-DN-C0204-013

February, 1975

MDAC

NAS 9-13970

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

A	Area
AFC	Automatic flight control
AMPS	Amplifiers
A_n	Acceleration, normal
C	Capacitance
CADC	Central Air Data Computer
CCATS	Command Communications and Telemetry System
CDP	Central Data Processor
CMDS	Commands
COND	Condition
CSM	Command Service Module
CTS	Control Transfer System
d	Distance
db	Decibel
dbw	Power in decibel relative to one watt
DDA	Digital differential analyzer
DDSU	Display Drive Select Unit
E	Permittivity
ECU	Electronic Control Unit
E_f	Energy of one spark discharge for flashover

E_o	Permittivity of free space
E_p	Energy of one spark discharge for punch-through
f	Frequency
FCC	Flight Control System
FO/FO/FS	Fail operational/fail operational/fail safe
ft	Feet
GHz	Gigahertz
GSC	Goddard Space Center
IC	Integrated circuit
ILS	Instrument Landing System
INS	Inertial Navigation System
INST	Instructions
IOP	Input output processor
IU	Instrument Unit
JSC	Lyndon B. Johnson Space Center
KHz	Kilohertz
KSC	John F. Kennedy Space Center
KV	Kilovolts
KW	Kilowatts
LCC	Launch Control Center
LH	Left hand
LM	Lunar Module

LVDA	Launch Vehicle Data Adapter
LVDC	Launch Vehicle Digital Computer
LVDT's	Linear variable differential transformers
LUT	Launch Umbilical Tower
m	Meter
MCC	Mission Control Center
MHz	Megahertz
MOCR	Mission Operations Control Room
MOS	Metal oxide silicon
MOSFET	Metal oxide silicon field effect transistor
MSBLS	Microwave Scanning Beam Landing System
msec	Milliseconds
MW	Megawatt
NASA	National Aeronautics and Space Administration
NM	Nautical mile
P	Precipitation
PAFAM	Performance and Failure Assessment Monitor
pk	Peak
PSU/SP	Parameter Setting Unit/Status Panel

Q	Charge in coulombs
R&D	Research and development
RF	Radio frequency
RH	Right hand
RSI	Reusable surface insulation
RTCC	Real Time Computer Complex
SAS	Stability Augmentation System
SIP	Strain Isolation Pad
sq. m.	Square mile
SYS	System
TACAN	Tactical Air Navigation
TAGS	Tactical Airborne Guidance System
TILS	Tactical Instrument Landing System
TM	Telemetry
TMR	Triple modular redundancy
TPS	Thermal Protection System

SYMBOLS

$\dot{\theta}$	Pitch rate
μ	Micro
μs	Microseconds
μV	Microvolts

SYNOPSIS

Generic design flaws of redundant computer systems can result in undesirable operation, such as monopolization of computer controlled data buses by a faulty element, accidental system shutdown due to transients, erroneous memory alteration, loss of control system equalization, and software oversights which can be common in all redundant strings.

History has shown that generic design failures have occurred on aerospace vehicles. On aircraft, these problems have resulted in simultaneous malfunctioning of multiple redundant computers requiring faultdown to the mechanical cable flight control system. The system features that cause generic design failures are susceptibility of electronic circuits to electromagnetic or electrostatic energy, susceptibility of interfacing parallel redundant electronic strings to multiple string failures, and computer programming oversights causing common failures within each string.

The low power solid state integrated circuit (IC) devices are much more susceptible to extraneous electromagnetic and electrostatic interference than their earlier counterpart, the discrete transistor. This means that special precautions must be taken to preclude generic design failures of these susceptible electronic components on the Shuttle. Analyses indicate that the Microwave Scanning Beam Landing System (MSBLS) ground station will most probably not interfere with the electronic circuits.

However, the high power AN/FPS-16 radar tracking system will interfere with the electronic circuits unless about 60 decibels (db) of attenuation (vehicle skin plus cable) to interference is achieved.

Experience has shown that vehicle skin will attenuate RF energy by about 15 db without special design considerations; while 40-45 db of skin attenuation can be achieved, (at least on small vehicles) with special design considerations. Braided type cable shielding can typically provide up to 30 db of shielding to RF energy with special design considerations (e.g. 360 degree seals, similar to waveguide connectors, at the connectors).

Lightning is, however, a more difficult noise source to protect against than radars. Shielding levels of 70 to 100 db are required to provide the most sensitive ICs protection against lightning.

The mechanism for pickup of electromagnetic energy is through external skin cracks (e.g. bolt holes even with bolts installed) and internal cable bundles. Therefore, better shielding of the black-box enclosure is generally of no help. No attempt was made in this report to estimate or calculate the amount of skin and cable attenuation to be provided by the current Orbiter design. However, cut-outs in the metallic skin that are fitted with low dielectric constant material for antenna windows could reduce the skin attenuation to near zero db, unless the design of the antenna and antenna system mounting structure precludes leakage of RF energy to the inside of the Orbiter. Skin with virtually no attenuation to RF radiation could make the Orbiter electrical components very susceptible to RF signals.

The Orbiter is judged uniquely vulnerable to electrostatic charge hazards because of the high electrical resistivity and large surface areas of its Reusable Surface Insulation (RSI) which is in proximity to inherently susceptible solid state digital avionics equipment. Additional NASA Avionics System Engineering Division effort has been initiated to further define this problem and to generate solutions.

An aircraft computer switching philosophy used on operational systems has been distilled by surveying existing systems. Key points of this philosophy are:

a) Plan for failures by using a deterministic design approach that assumes failures will happen (Murphy's Law). Do not rely on a reliability number (such as .9998) alone.

b) Functional redundancy is preferred to hardware redundancy only.

c) Reconfigure by turning devices off rather than on.

d) Avoid synthesis of a viable system from several strings. The pilot needs an easily understandable equipment configuration. Ease of understanding is best achieved by switching entire strings of electronic equipment.

e) Confirm failures before disconnecting equipment when possible to preclude using up configuration options too fast and to allow the crew to function in the decision process.

f) Permit several levels of degraded performance to preclude using up options too fast.

Items a) thru d) appear to be applicable to the Orbiter while e) and f) may not be applicable due to the greater time criticallity of the Orbiter functions and the higher Orbiter performance requirements.

Table IV on page 20 provides a summary of computer switching approaches for some of the existing aircraft and spacecraft systems surveyed. It was found that most systems are designed to prohibit generic failures and/or are not similar enough to the Shuttle systems to merit further study. This is indicated from the following system characteristics.

a) Some systems use dedicated computers for different functions.

b) Many systems are simplex in nature.

c) Some systems use manual break-before-make switching for computers.

d) Many systems are all analog in nature and many use no data buses.

It was found that the airborne systems were more applicable than the ground systems. In particular the DC-10 with its functional redundant performance and failure assessment monitor (PAFAM) system and the S-3A with its cross strapped computer systems, are of interest.

Examples of: computer system shutdowns due to transients, errors in parallel computational strings due to failures of interfacing elements, and multicomputer shutdowns due to computer programming oversights were found in the course of this study. However, no examples were found of monopolization of data buses or erroneous memory allocation due to generic system failures.

No aircraft systems were found that use an integrated data bus approach to handle both flight critical functions and most other major vehicle functions, as done on the Orbiter. The only aircraft found that plans to use a fly-by-wire control system in its operational phase, without the availability of a mechanical cable backup flight control system, is the new YF-16 light weight fighter aircraft. This aircraft has been flown hundreds of flights without accident due to failure of the all electronic flight control system.

1.0 Introduction

This study was conducted at the request of and under the direction of the NASA Avionics System Engineering Division. The purpose of the study was to investigate multi-computer configurations and redundancy management techniques to determine methods to prevent and/or treat generic design flaws. For the purpose of this report generic design failures are defined as undesirable operations of redundant computer configurations which are typified as follows:

- monopolization of all or many data buses by a faulty computational element in one or more strings
- accidental subsystem/system shutdown due to transients
- erroneous memory alteration (overlay) due to crosstalk between computers
- loss of control equalization where equalization is required for normal operation
- software oversights which can be common in all redundant operational strings

This report covers the first portion of the psychotic computer study in which generic flaws are defined and the prevention and treatment of generic design failures are discussed. The computer configurations and redundancy management of existing aircraft, spacecraft, and industry computer systems are also reviewed. The purpose of this review is to assimilate the best existing computer system philosophy guidelines for use on the Shuttle program. The existing systems are investigated to determine computer redundancy configurations, redundancy switching criteria, and immunity to generic design flaws.

The second portion of the generic design flaw study is to include an Orbiter redundant computer analysis to define and solve specific Orbiter generic design problems. This portion of the study is to be conducted after completion of this report with the results being in a separate report.

This report is mainly comprised of information previously published in preliminary working papers. The source of data for this report includes both written reports from and telecons with the appropriate companies and engineering staffs responsible for the investigated aircraft, spacecraft, and industrial computer systems. Written references used are included in the list of references.

History has shown that computer generic design flaws have occurred on aerospace vehicles. On aircraft these problems have resulted in malfunctioning of the multiple redundant computer systems requiring faultdown to the mechanical cable flight control system. For example, on TAGS (Tactical Airborne Guidance System) the entire computer system (three computers) shut down due to a software design oversight requiring reversion to mechanical cable flight control to preclude a crash. The software was not designed to handle a second computer failure before three computer computational cycles elapsed due to an oversight in the computer program design. On the DC-10 the quad redundant analog flight control system comparators were unable to detect a bias in the yaw flight control channel since all channels included the bias due to a part failure and a design weakness. However, an independent monitor system, the performance and failure assessment monitor (PAFAM), detected this generic failure allowing manual takeover using the mechanical cable system. These generic failure examples were found in the course of this study and do not represent a complete listing. Other failure examples are included in other report sections. A special survey to find failure examples was not made since the time to document more failures was not felt to be warranted and in most instances manufactures are reluctant to release any information regarding failures of their systems.

Examples of: computer system shutdowns due to transients, errors in parallel computational strings due to failures of interfacing elements, and multicomputer shutdowns due to computer programming oversights were found in the course of this study. However, no examples were found of monopolization of data buses or erroneous memory allocation due to generic system failures.

No aircraft systems were found that use an integrated data bus approach to handle both flight critical functions and most other major vehicle functions, as done on the Orbiter. The only aircraft found that plans to use a fly-by-wire control system in its operational phase, without the availability of a mechanical cable backup flight control system, is the new YF-16 light weight fighter aircraft. This aircraft has been flown hundreds of flights without accident due to failure of the all electronic flight control system.

The terms "generic design failures" and "generic design flaws" used in this report are considered to be synonymous with the terms psychotic operation/behavior and psychotic problems respectively. These alternate terms have been used in some of the earlier working papers on this same subject.

Paragraph 2.0 of this report discusses design features that are subject to generic design flaws and Paragraph 3.0 includes a summary of philosophy items, pertinent to the Space Shuttle Orbiter, that were obtained from an investigation of existing computer systems. Paragraphs 4.0 and 5.0 include the recommendations and conclusions. The Appendices include more detailed information on electrostatic interference and additional and more detailed information on individual computer systems investigated.

2.0 Design Features Subject to Generic Design Failures

Before investigating existing computer systems, a brief look into system design features that are subject to generic design failures and design practices that can alleviate chances of these failures is in order. Integrated circuit (IC) components, interfacing parallel redundant strings, and computer programs can all be subject to generic design failures.

Additional hardware and software redundancy of identical design will normally not help to reduce the generic design failure effects. This is due to the generic nature of these failures which affect more than one or all of a given type of line replaceable units simultaneously.

2.1 Integrated Circuits

Digital avionic systems employing efficient, but low power solid state IC devices are much more susceptible to extraneous electromagnetic and electrostatic interference than their earlier counterpart, the discrete transistor. This demands that engineering design attention be given to natural and manmade environmental disturbances to negate the effects of these disturbances on very sensitive IC devices.

Figure 1 and Table I indicate that the semiconductor development trend is toward increasingly lower power operating levels and greater noise sensitivity as the population of active elements per unit area of substrate becomes larger. Vulnerability to high voltage, low energy transients is also indicated by the fact that factory personnel working with IC devices are often required to wear wristband grounds to avoid equipment burn-out from discharge of clothing charges.

2.1.1 Electromagnetic Sources of Interference

Two prime examples of extraneous electromagnetic sources that can affect sensitive solid state IC devices are ground radar scanning of the Shuttle and lightning strikes. Both of these interference sources are difficult to control and require consideration of sufficient shielding in the system design.

2.1.1.1 Electromagnetic Energy Transfer Mechanism

A manner in which radiated energy can get into IC devices is as follows. Radiated energy impinging on the vehicle penetrates through the surface via cracks, bolt holes (with bolts installed) or other openings. Once the energy has penetrated the vehicles' outer skin the avionic cable bundles act as an antenna. The cables serve as a transducer, which changes radiated energy to conducted energy, which is then conducted to the IC devices.

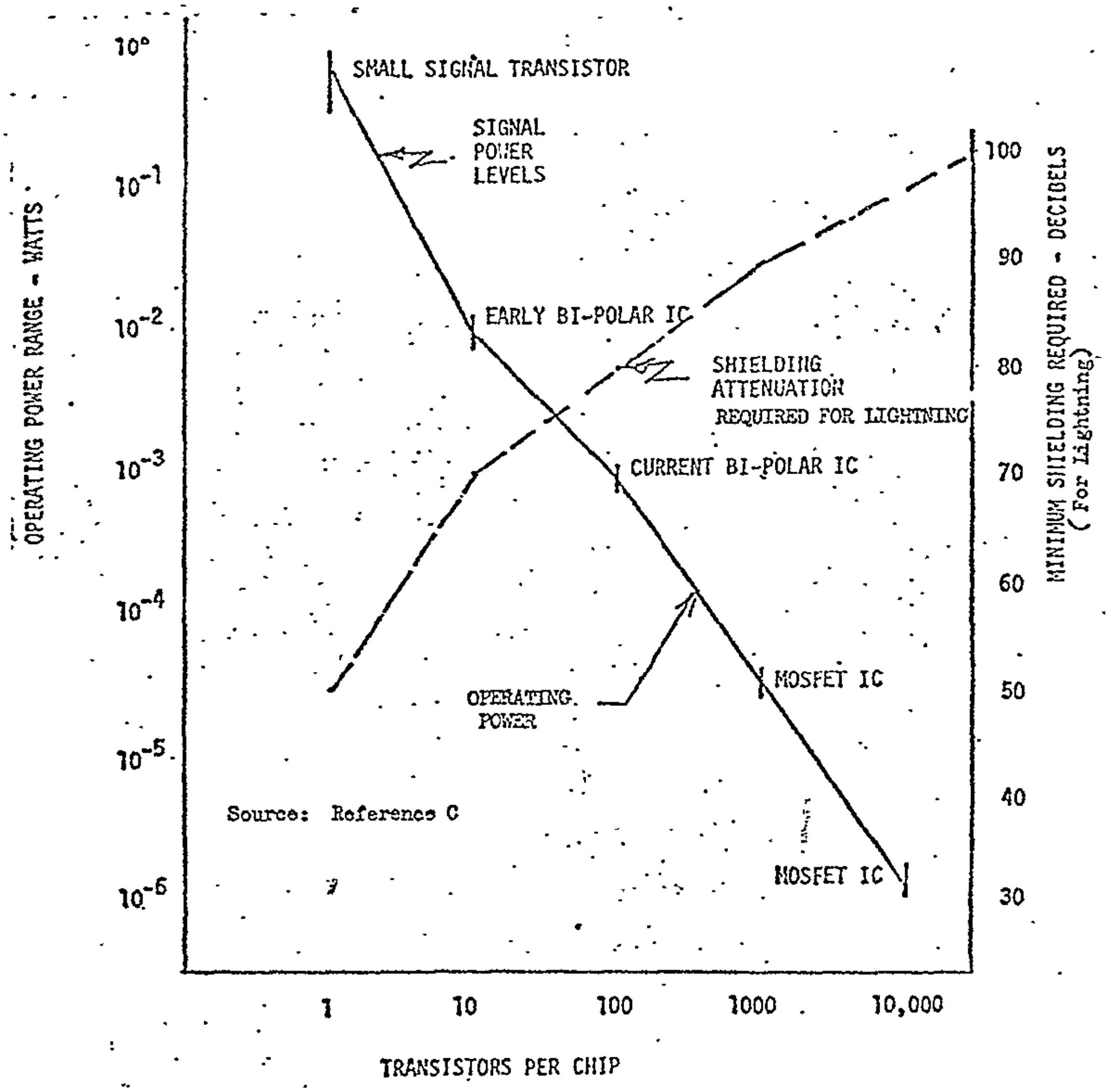


FIGURE 1 - SEMICONDUCTOR DEVICE OPERATING LEVELS

TABLE I

ELECTRONIC DEVICE SUSCEPTIBILITY LEVELS

DEVICE	MALFUNCTION LEVEL	BURNOUT LEVEL
Transistor	$\gtrsim$ 50 millwatts	50 watts (MDC test data)
Typical Integrated Circuit	$\gtrsim$ 10 to 100 milliwatts	(not determined)
MOSFET Integrated Circuit	0.3 to 3 microwatts (estimated)	4 to 40 milliwatts (estimated)

An unblemished skin (no fasteners, no cracks, or openings) typically provides approximately 100 db of isolation to RF energy. However, an unblemished skin is virtually not practicable It has been found that the bolt holes with bolts installed and tightened firmly, reduces skin shielding from about 100 db to about 40 db. On such programs as Gemini and Harpoon Missile, it was found through tests that the external skin provided little attenuation (typically 10 to 15 db) to radiated energy impinging on the vehicle without specifically designing for RF protection. These tests were performed in the 3 to 9 GHz range.

Skin shielding could be as low as zero decibels if dielectric windows for sensors are employed. On the Harpoon Missile, the surface was radiation sealed by using special gaskets and processes to increase the RF attenuation produced by the skin. Skin attenuation was increased from 10-15 db to 40-45 db. Braided type shields on avionic cables can typically provide from zero to 30 db of shielding to RF energy depending on the shielding design. This shielding adds to the attenuation provided by the skin. On the Harpoon Missile it was found that to achieve 20 to 30 db of attenuation from braided shielding required a 360 degree seal, similar to waveguide connectors, at the connectors.

Thirty db of skin attenuation plus 30 db of cable attenuation would provide enough isolation to be effective against most radars as indicated in the following paragraphs. Greater isolation, however, may be required for lightning.

2.1.1.2 Effects of MSBLS and AN/FPS-16 Radar

The Shuttle relies on ground generated RF signals from the MSBLS for automatic landing; and it is highly desirable to track the Shuttle with surveillance radars at least during ascent and landing.

Table IIa indicates that the radiated power from the ground MSBLS/Tactical Instrument Landing System (TILS) station, seen at the Orbiter, is in the microwatt range. Figure 1 indicates that the most sensitive MOSFET IC's also operate in the microwatt range. Therefore, to preclude circuit malfunctions, with a 10 db margin of safety, due to the MSBLS ground radiated power, would require 10 db of RF isolation. This 10 db of isolation should be easy to achieve as indicated in the above paragraphs.

Table IIb indicates that the maximum radiated power from the AN/FPS-16 radar, seen at the Orbiter, is in the milliwatt range. This would require attenuation of about 60 db, vehicle skin plus cable, to assure satisfactory operation of the most sensitive IC devices, assuming a 10 db margin of safety. Note, that this is for the Orbiter at one nautical mile from the radar and that the attenuation required would decrease by 6 db each time this range is doubled.

The MSBLS ground station and the AN/FPS-16 radar were selected

TABLE II

RADAR INTERFERENCE SOURCES

a) MSBLS/TILS Interference Sources

	MSBLS/TILS Transmitter Power (2KW pk)	33dbw
	MSBLS/TILS Transmitter Antenna Gain, Ground	29db
	Free Space Loss (15.3GHz, 1NM)	- 121db
*	Power Received at the Shuttle at 1NM range	- 59dbw
		or 1.25×10^{-6} watts

b) AN/FPS-16 Radar Intereference

	AN/FPS-16 Transmitter Power (1.0 MW pk)	60dbw
	AN/FPS-16 Circuit Losses	- 2db
	AN/FPS-16 Antenna Gain	45db
	Free Space Loss (5.6 GHz, 1NM)	- 113db
**	Power Received at the Shuttle at 1NM range	- 10dbw
		or $100,000 \times 10^{-6}$ watts

Notes:

* Flux density of 0.037 watts/sq. m. at Orbiter

** Flux density of 465 watts/sq. m. at Orbiter as examples to determine if such ground based radiators could possibly cause Orbiter circuit malfunctions. It appears that high power radars could cause circuit malfunctions if sensitive electronic circuits are used and if the Orbiter skin and avionic cable bundles provide low attenuation to RF energy. A more detailed analysis of all radiation sources that may irradiate the Shuttle, and an analysis of Orbiter skin and cable bundle attenuation to RF energy would be required to determine the impact of ground radar scanning the Shuttle Orbiter.

2.1.1.3 Effects of Lightning

Table III indicates that high shielding levels (70-100 db) are required for IC protection against lightning.

Few serious accidents on commercial aircraft have been attributed to lightning because they have heavy metallic surfaces, inherent flight stability, and safety of flight control systems free of susceptible avionic components. The Orbiter is inherently unstable and it has not been demonstrated as yet that the system is free of susceptible avionic components. Therefore, the effects of lightning strikes on flight control functions should be considered in detail on the Shuttle.

2.1.2 Electrostatic Sources of Interference

In addition to electromagnetic energy sources there are electrostatic charge and discharge mechanisms that have resulted in a variety of problems on aerospace vehicles. The Shuttle

TABLE III

COMPONENT SUSCEPTIBILITY TO LIGHTNING

DEVICE	Minimum Shielding Required to Protect Against Lightning
Bipolar Integrated Circuits (100 transistors per chip)	70db
MOS (unipolar) Integrated Circuits (5000 to 10,000 transistors per chip)	100db

Orbiter is judged uniquely vulnerable to electrostatic charge hazards because of the high electrical resistivity and large surface areas of its RSI which is in proximity to inherently susceptible solid state digital avionics equipment.

Exploratory laboratory tests and analytical predictions of RSI electrostatic behavior suggests a much more severe impulse noise environment for the Orbiter than commonly experienced in flight on conventional metallic skinned airplanes. The electrostatic potential is acquired through frictional charging by particulate matter in the atmosphere (principally ice or rain particles in clouds), by engine exhaust charging, or by thunderstorm cross-fields. Conventional aircraft use sharply pointed "static dischargers" located in high aerodynamic flow regions near the extremities of the aircraft to bleed off excess charge in a controlled manner, virtually eliminating the electrostatic interference problems. Without the dischargers, the static charge may build up until the vehicle is charged to a very high potential; on the order of hundreds of thousands of volts. However, with static dischargers and conventional metal structures, the charge rapidly bleeds off and maintains the vehicle at an acceptable low voltage level.

Two problems are immediately obvious in the Orbiter design with its dielectric (electrically insulated) RSI coating. The first is that static charge will build up on the dielectric surface and cannot bleed off because the dielectric will not conduct the charge to a common discharge point where a static discharger can be located. With the smooth contours of the RSI and the large surface area, voltages may build up on the exterior surface in the megavolt range with very significant energy. The second problem is the design of static dischargers which can withstand the dynamic launch and entry heating environments.

RF interference due to uncontrolled static charge results in precipitation--static in radios as well as logic errors in digital circuits. Flights of both the Minuteman and the Titan have shown that airborne computers used for guidance and commands are extremely susceptible to a single discharge of very low-energy static electricity. See Appendix I for a more thorough description of: avionic responses to a precipitation static environment, other threats from electrostatic charges, and electrostatic noise spectrum and magnitudes.

2.2 Interfacing Parallel Redundant Electronic Strings

Multiple computational strings often interface at comparators/voters and in equalization circuits. Some typical development practices which help to preclude generic failures due to such interfaces are:

a) Comparators that are comparing computations from more than one channel should have failure modes such that a failure is obvious. A "fail obvious" comparator is needed.

b) Whenever information from two channels flows within the same box (e.g. information to comparators), wiring and connector pin separation should be such that the two lines cannot be shorted together. Shorts between two channels should not go undetected.

c) Comparisons should be made at the end of the control strings. However comparisons can also be made at other points.

d) Recognize that failures can be altitude or other flight parameter sensitive. For example, a failure may be simulated at 100 feet altitude with no deleterious effects; but at 300 feet altitude, the failure could cause catastrophic effects. This is because the failed condition is present for a longer period of time before landing.

Techniques used for equalization of commands in the parallel and redundant computational strings are of prime concern on the Orbiter. This is because small differences in signals between computational strings have a tendency to propagate and result in divergent commands because of integration processes in the system. This divergent tendency can be overcome by proper equalization and/or synchronization techniques. However, these techniques tend to add complexity, reduce reliability, and add computational string interface points that are subject to generic design failures. Therefore, it is important that the final solution to the equalization problem be proven free of generic design flaws.

2.3 Computer Programming

In addition to normal computer program verification,the following verification techniques should be used to lessen chances of psychotic operation due to computer programming oversights.

a) Verify effects of sequences or strings of failures. On past programs (e.g. TAGS) certain timing of failures relative to each other have caused shutdown of all computer systems. All possible reversionary modes and their effect must be investigated.

b) Pay particular attention to those computations that are not performed every computational cycle. The effect of errors in these computations tend to be overlooked.

c) Verify times for which computers will wait for data. For example: are there instances in which one or more computers could be running with old data and one or more other computers running with newer data? This could cause comparators to indicate a non-compare.

d) Recognize that checking out the computer program is different from checking out the system design—both are required.

3.0 Philosophy Items of Existing Computer System

3.1 Aircraft Computer System Philosophy

Both flight and non-flight computer systems were investigated. However, the airborne systems were found to have more applicability to the Orbiter computer systems than the ground based systems. A computer system design and switching philosophy was generated from the information received. It is felt that this philosophy represents typical computer switching philosophy for existing operational aircraft. Key points of this philosophy are:

a) Plan for failures by using a deterministic design approach that assumes failures will happen (Murphy's Law). Do not rely on a reliability number (such as .9998) alone.

b) Functional redundancy is preferred to hardware redundancy only.

c) Reconfigure by turning devices off rather than on.

d) Avoid synthesis of a viable system from several strings. The pilot needs an easily understandable configuration. Ease of understanding is best achieved by switching entire strings of electronic equipment.

e) Confirm failures before disconnecting equipment when possible to preclude using up configuration options too fast and to allow crew to function in the decision process.

f) Permit several levels of degraded performance to preclude using up options too fast.

These system philosophy points are used for current commercial and military aircraft and therefore are not necessarily applicable to the Shuttle Orbiter. However, items a) thru d) appear to be applicable to the Orbiter while e) and f) may not be applicable due to these greater time criticality of the Orbiter functions and the higher Orbiter performance requirements. This section of the report discusses only the key findings from the survey of existing computer systems. For additional information on individual computer systems refer to Appendices II through XVIII.

3.2 Aircraft Computer System Overview

An overview of key parameters of existing systems is given in Table IV. Included in the overview are parameters that are of interest in the generic design flaw investigation. These parameters include failure cues provided to the pilots, criteria used to deactivate failed computers, methods used for system reconfiguration, and the "state" assumed by a failed computer.

Large commercial and military aircraft investigated (DC-10, L-1011 and B-1) use four computational strings. The four computers are grouped into two pairs to form a dual-dual computational system. This is done to keep one group of two computers physically and electrically isolated from the other group. That is, the computer one output is compared with the computer two output

TABLE IV - COMPUTER SWITCHING APPROACHES

TYPE OF COMPUTER SYSTEM	FAILURE CUES TO PILOT	CRITERIA TO DEACTIVATE FAILED COMPUTER	METHOD OF RECONFIGURATION — MANUAL/AUTO	FAILED COMPUTER CONTINUES TO OPERATE
DC-10 2 BY 2 COMPUTER COMPARISON PLUS PERFORMANCE AND FAILURE ASSESSMENT MONITOR (PAFAM).	AMBER LIGHT— ONE HALF SYSTEM FAILED. RED LIGHT— COMPLETE SYSTEM FAILED.	NON COMPARE OF STRINGS— PAFAM INDICATES FAILURE.	AUTOMATICALLY GOES TWO STRINGS. PAFAM PREVENTS AUTOLAND DISCONNECT IN SOME CASES. PAFAM NOTIFIES CREW OF FAILED COND.	YES
L1011 2 BY 2 COMPARISON OF ANALOG STRINGS PLUS VOTERS FOR SIGNAL SELECT. VOTERS SELECT ONE SIGNAL TO DRIVE VEHICLE.	BAT HANDLES DROP IF FEEDBACK FROM SERVOS INVALID. "NO DUAL" OR "DUAL AUTOLAND NOT AVAILABLE" DISPLAY.	NON COMPARE OF CHANNELS & INVALID SERVO FEEDBACK.	AUTOMATIC DISCONNECTION SWITCH OUPUT OF AFC TO GROUND POINT. CREW NORMALLY ONLY MONITORS.	YES
B1 2 BY 2 COMPARISON OF ANALOG STRINGS.	PILOT NOTIFIED OF NON COMPARE OF COMPUTATIONAL STRINGS.	IN AUTOLAND MODE: WITH SINGLE FAILURE PILOT GOES MANUAL OR ABORTS LANDING.	AUTOMATIC DISCONNECTION. PILOT CAN RECONNECT STRING IF FAILURE INDICATION FOLLOWED BY GOOD INDICATION.	YES

ORIGINAL PAGE IS
OF POOR QUALITY

TABLE IV - COMPUTER SWITCHING APPROACHES (COMPLETED)

TYPE OF COMPUTER SYSTEM	FAILURE CUES TO PILOT	CRITERIA TO DEACTIVATE FAILED COMPUTER	METHODS OF RECONFIGURATION—MANUAL/AUTO	FAILED COMPUTER CONTINUES TO OPERATE
F-4 AUTOLAND SIMPLEX AUTOLAND AUTOPILOT COUPLER (SPN-42).	DEDUCED FROM SECONDARY SYSTEM (SPN-41), "MANUAL" OR "WAVEOFF" COMMANDS. MASTER CAUTION AND COUPLER OFF LIGHTS.	NO CMD'S RECEIVED FOR 'X' TIME, HARDOVER CONTROL SURFACE, AIRCRAFT OUTSIDE SAFE BOUNDARIES SET BY GROUND.	AUTOMATIC	YES
F-15 SIMPLEX COMPUTER WITH TWO DATA BUSES (NOT IN SAFETY OF FLIGHT LOOP).	PANEL LIGHT ALERTS CREW.	PILOT MAKES DECISION.	MANUAL	YES
F-4 FLY BY WIRE. NO AUTOMATIC FLIGHT MODES OR COMPUTERS	PANEL LIGHTS INDICATE FAILED ELECTRONICS AND FAILED ACTUATORS IN EACH AXIS AND EACH STRING.	FAILURES DETECTED BY COMPARATORS DEACTIVATE ELECTRONICS AND/OR ACTUATORS.	AUTOMATIC	YES, FAILED ELECTRONICS OUTPUT IS SHUNTED TO GROUND.
SATURN V/ INSTRUMENT UNIT (IU) SINGLE COMPUTER WITH DUPLEX MEMORY & TMR CIRCUITRY	PILOTS RECEIVE ATTITUDE OF BOOSTER.	ONLY INPUTS TO THE TMR LOGIC THAT DO NOT COMPARE ARE NOT USED.	MAN NOT INVOLVED. COMPUTER TRYS TO REINITIALIZE.	YES, HOWEVER FAILED INPUTS TO THE TMR LOGIC ARE NOT USED.

and the computer three output is compared with the computer four output. There are no or few connections between groups of strings. Computers one and two form a group, and computers three and four form another group.

The DC-10 equalizes, or makes equal, the sensor signals feeding each group of computers. This is accomplished in a manner necessary to cancel long term variations but detect short term variations between the channels in a group. These short-term variations are more indicative of failures. Similarly the computational difference between the two channels under comparison are subtracted out (cancelled) so that the comparators will only sense true failures.

The PAFAM used on the DC-10 was not used in the other aircraft systems. The PAFAM provides supervisory control of autoland disconnect functions and includes a fast time model for predicting the aircraft touchdown point. The PAFAM has been found useful but not mandatory for autoland.

On the DC-10 program, it has been indicated that two types of system degradations must be designed for: equipment malfunctions and input source errors. Input source errors include wind sheers and erroneous landing system information. The PAFAM was used to detect these input source errors and to provide predicted ground landing system data during short drop outs or losses of ground landing system information.

All of the large operational military and commercial aircraft use a fly-by-cable backup system for flight control. The F-8C test aircraft was the first (1972) aircraft to fly with a fly-by-wire system with no mechanical backup system for failure reversion. This was on a test system only. The new YF-16 is believed to be the first fighter with no mechanical cable backup system in its planned operational configuration. In all cases it was found that a failed computer was allowed to continue to operate after it was switched off line. In the event the failure is rectified the computer could then be used again.

Numerous methods of reconfiguring computer systems were noted. The switching of a computer off line was accomplished automatically, manually and sometimes a combination of automatic and manual techniques were used. Some of the methods of reconfigurations found are defined in Table IV.

The fighter aircraft computer systems were generally not applicable to the Orbiter because often simplex dedicated computational strings are used for each group of functions. In the F-15 the simplex computation string, performing non safety of flight computations, can however be pressed into service to perform navigation computations if required as a backup measure.

3.3 Spacecraft Computer System Overview

The Saturn V Instrumentation Unit did not include any means for the crew to manually reconfigure the Instrumentation Unit computer system due to lack of redundancy and time criticality of the booster functions.

A primary example of how functional redundancy has been used on spacecraft programs is the use of the Lunar Module (LM) guidance system to safely bring the combined Command Service Module (CSM) and LM back to Earth after a failure in the Apollo 13 CSM.

3.4 Ground Computer System Overview

Review of the ground computer systems indicated that these systems were not applicable to the Shuttle application. This is because most of these systems used dedicated strings and manual break-before-make switching. It has been found that the typical failure is a computer malfunction that manifests itself in large errors such that the operator can detect the errors and effect a manual switch over to a backup computer. The break-before-make switchover does not allow for generic failures per the definition used in this report. The ground computer systems reviewed included the NASA JSC mission control center (RTCC and CCATS) computers, the NASA GSC remote site automated systems, and the KSC Saturn Launch Vehicle (PAD39) automated systems. See Appendices II through XVIII for further definition of the computer systems investigated.

4.0 Recommendations

It is recommended that no further studies of the existing aircraft, spacecraft, and ground systems be undertaken unless they are of a very specific nature to investigate individual items for which information is required. It is felt that the review of existing systems has provided some general computer system design philosophies and general guidelines which are applicable to the Shuttle Orbiter and which have been enumerated in this report. However, it has also been found that most systems implementations reviewed can only provide a limited amount of applicable information due to their dissimilarity to be Shuttle Orbiter.

It is also recommended that the emphasis now be directed towards the Shuttle to relate the applicable aircraft philosophies, to study applicable equalization approaches and to investigate individual potential generic failure problems of the Orbiter.

It is further recommended that design groups be made aware of their responsibility to stamp out generic failure mechanisms by checking their designs for possible generic failure modes and by eliminating any failure mechanisms found. However, it must be recognized that this effort can only be directed from a system design team having cognizance of the Shuttle systems as well as the generic failure mechanisms.

It is also recommended that efforts to assess the susceptibility of the Orbiter to electromagnetic and electrostatic energy be continued and increased in order to solve the apparent generic design failure modes due to these energy sources. None of the existing aircraft electrostatic dischargers, either active or passive are likely to meet the Orbiter requirements as they are designed. Therefore, new or modified designs are recommended.

5.0 Conclusions

It is felt that this investigation has been of value and that it will provide background material necessary to identify, define and solve unique Orbiter generic design problems.

In many areas much additional work remains. For example:

- The potential for Shuttle Orbiter generic design failures due to electromagnetic or electrostatic energy was proven. However, the unique transfer functions for the coupling of this energy into the Orbiter circuit components and the susceptibility of these components were not determined..
- The design features and philosophy of some existing computer systems have been determined. Now these philosophies need to be directed toward the Shuttle, so that they can be used where appropriate.
- The susceptibility of interfacing parallel redundant strings of electronics and computer programs to generic failures have been identified. Detailed effort is now required to analyze all interfaces of parallel redundant strings including interfaces for signal equalization, voting, and comparisons. Effects of synchronization, voting, isolation, disconnect method, signal bias, time delays, asynchronous operation, and inadvertent errors/failures must be evaluated.
- Programming rules and tests to minimize or eliminate programming oversights need to be defined and implemented.

REFERENCES

1. Deets, Dwain A., "Design and Development Experience with Digital Fly-By-Wire Control Systems in an F-8C Airplane", included in the NASA Conference Report titled, Advanced Control Technology and its Potential for Future Transport Aircraft, July 9-10-11, 1974, Los Angeles, Calif.

2. Lock, William P. and William R. Petersen, "Mechanization of and Experience with a Triplex Fly-By-Wire Backup Control System", included in the NASA Conference Report titled, Advanced Control Technology and its Potential for Future Transport Aircraft, July 9-10-11, 1974, Los Angeles, Calif.

3. Hooker, David S., "Survivable Flight Control System", Interim Report No. 1 Studies, Analyses and Approach, AFFDL-TR-71-20, May 1971.

4. Lockheed Electronics Company, Inc., "Applicability of S-3A and C-5A Data Management Systems to Phase B Space Shuttle Requirements", LEC 26-439-111, January 1972.

5. IBM, "TAGS Redundancy Management", Final Report, 72-156-68, 29 December 1972.

6. Anderson, C. A., "Development of an Active Fly-By-Wire Flight Control System", included in the NASA Conference Report titled, Advanced Control Technology and its Potential for Future Transport Aircraft, July 9-10-11, 1974, Los Angeles, Calif.

7. NASA, Saturn V Flight Manual SA509, MSFC-MAN-509, 15 August 1969, changed 1 January 1971.

APPENDICIES

Appendicies I through XVIII follow. Appendix I includes more detailed information on electrostatic interference and Appendicies II through XVIII include additional and more detailed information on individual computer systems investigated.

APPENDIX I

ELECTROSTATIC INTERFERENCE

1.0 Avionic Responses to Precipitation Static Environments

1.1 RF Interference

Radio frequency interference due to static charge has been encountered since the first flights of early aircraft in bad weather. Precipitation static (P-static) is well understood today and has become the subject of specifications that control both the charging of the source and the susceptibility of radio equipment. Nevertheless, P-static control remains an active discipline as the evolution toward more complex, more sensitive avionics systems continue to uncover new modes of interference. Phase-lock systems, FM systems, radio-guidance systems, and navigation aids are all affected by static electrification discharges through different interference modes. Much recent attention has been directed toward quantifying the acceptable interference level in terms more appropriate for systems than the simple signal power/noise parameter. Expressions for the bit rate error and the probability of a loss of phase lock, and techniques to reject unreasonable data have been developed.

1.2 Logic Errors

Logic errors caused by a single discharge of static electricity have been encountered when using computers for guidance, navigation, and sequencing and in logic based programs for telemetry and data acquisition systems. This type of interference is quite a different matter than RF interference discussed previously. Airborne computers, widely used for guidance and commands, are extremely susceptible to a single discharge of very low-energy static electricity.

During early Minuteman test flights, single electrostatic discharges caused bit errors in the guidance computer, resulting in the loss of two missiles due to premature flight termination.

Single discharges of static also occurred on two separate Titan III flights in the late 1960s. In the first flight, a computer instruction was altered and the computer jumped into a backup flight mode. There were ten other modes it could have entered, any of which would have terminated the flight. On the next flight, steering data were altered and the missile turned off path; the guidance error introduced by the electrical discharge was eventually corrected. During an extensive ground test program that ensued, it was discovered that a spark energy as low as 565 ergs (0.0000565 joule) was sufficient to upset the computer. For comparison, an operating room is considered ether-safe at 40,000 ergs, and safe for the most sensitive anesthetics at 4,000 ergs.

Other computers of quite different and more advanced design were tested during a subsequent program. Despite the fact that these designs included isolators and filters on input-output lines, it was still found that some circuits were susceptible to as little as a few thousand ergs in a single spark. In one case, there was a period of 187 microseconds during certain logic operations in which the susceptibility was an order-of-magnitude more severe than at other times.

A similar situation has been encountered with data multiplexing systems. In one particular case, one of the wires was found susceptible to a few hundred ergs in discharge, and to an energy as low as 1 millivolt at a 100 kc rate. This wire was the midpoint connection between a balanced bipolar power supply and the differential (operational) amplifiers used to amplify all samples of data.

Finally, a very simple operational amplifier, used in an ordinance circuit monitor to ensure that there are no stray signals, has been found to be susceptible to a single static electricity discharge of 1 x 10^6 ergs applied in the positive sense, but susceptible to as little energy as 500 ergs applied identically, except in the negative sense.

2.0 Effects of a Static Environment on Non-Avionics

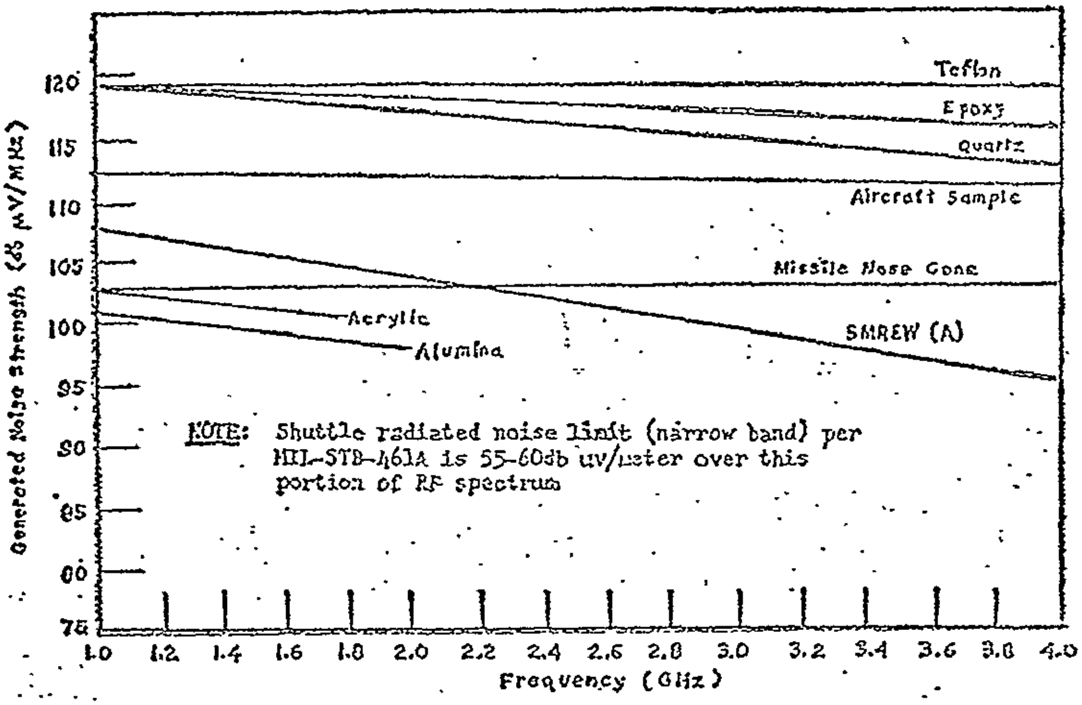
In addition to the interference with electronics the electrification of the Orbiter may pose a significant threat to the integrity of the RSI itself as well as a safety hazard to both ground and orbital operations. On conventional large aircraft, dielectric surfaces no larger than a windshield or canopy have proven very troublesome because of charge buildup. The charge often builds up until large sparks are generated to the surrounding metallic structure; or when metallic heaters are laminated into the windshield, sparks have punctured the outer laminates and attached to the heater circuit, often damaging both the windshield and heater circuit in the process. Charge can be stored long enough for serious electrical shocks to be experienced when ground personnel contact the windshield after landing. Obviously, these problems will be magnified greatly when essentially the entire exterior surface of the vehicle is non-conducting.

It is interesting to note that studies on the electrification of Titan and Apollo rockets have shown that the vehicle may be charged to several hundred kilovolts by engine exhaust charging once the exhaust plume breaks contact with the ground. Very little precipitation charging of these metal-skinned rockets was experienced at higher altitudes because the conductive exhaust bled the charge off the vehicle as fast as it accrued. This is unlike aircraft where the exhaust is not as conductive. It should also be noted that the polarity of static electrification is not usually predictable. It is, therefore, entirely possible that engine exhaust charging could raise the potential of the metal Orbiter substructure to a high value of one polarity, while an opposite precipitation charge develops on the RSI surfaces. The charges could not cancel, as they have been seen to do on conventional rockets, resulting in an additional potential difference between the exterior surface and the metal substructure.

Under these conditions the voltage differential can quickly become great enough to flash across the tile surface and discharge to the vehicle substructure via the gap joints. With the massive amount of dielectric RSI surface, charge accumulation may be rapid enough (with no bleed-off path) to result in a nearly continuous arc streaming across and through the tiles. Multiple pits and cracks in the RSI and its surface coatings are likely consequences of such an energetic sparking activity.

3.0 Electrostatic Noise Spectrum and Magnitudes

Both flight test and laboratory measurements of the precipitation static energy distributions have been made by a number of researchers in this field. Figure 2 shows the generated noise strength from laboratory simulated trioelectric charging of various dielectric materials in the one to four GHz frequency spectrum. The levels are high enough to suggest consideration be given to obtaining similar data for the Shuttle Thermal Protection System (TPS) materials, in view of a possible degrading influence upon TACAN, Radar Altimeter, and MSBLS performance during the landing phase. Figure 3 shows the noise current spectral density at lower frequencies as a function of altitude. Here it is significant to note a five fold buildup in noise at 1 MHz (Shuttle Data Bus Frequency) from sea level to 50,000 feet.



NOTE: Shuttle radiated noise limit (narrow band) per MIL-STD-461A is 55-60db uv/meter over this portion of RF spectrum

FIGURE 2 - GENERATED NOISE STRENGTH VS FREQUENCY

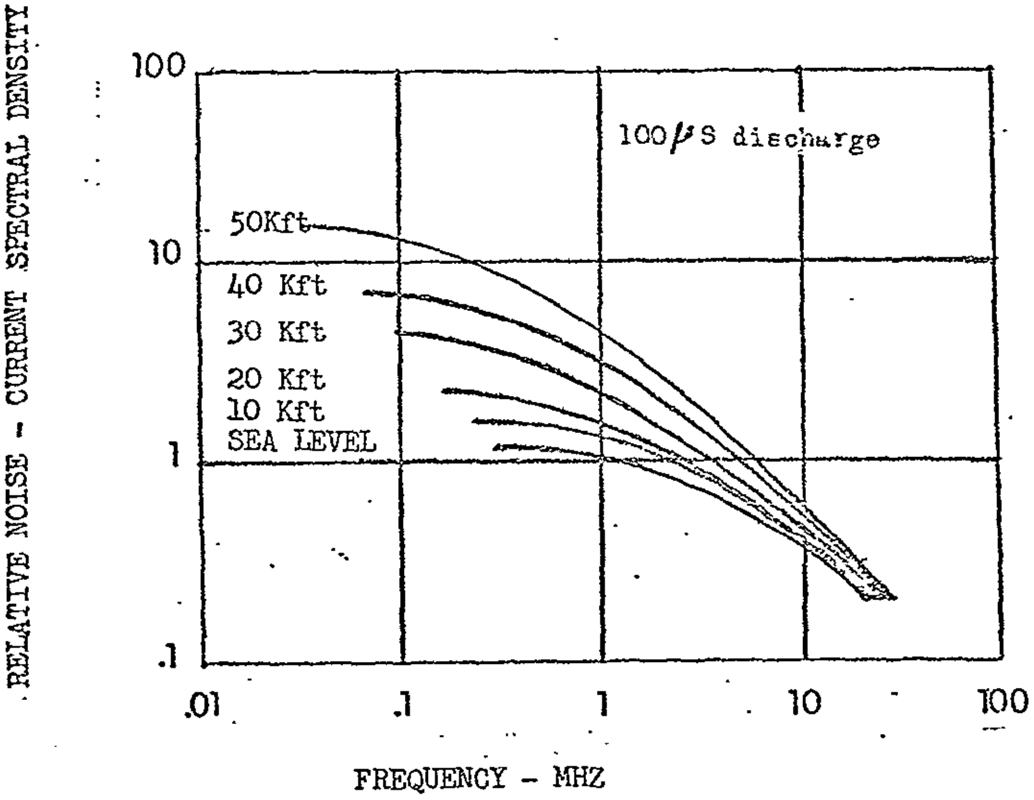


FIGURE 3 - NORMALIZED NOISE SPECTRUM FROM AIRCRAFT TRAILING EDGE

3.1 Preliminary Shuttle TPS Electrification Prognosis

During early experiments at the MDC Lightning Simulation Lab on the electrification characteristics of LI1500 RSI tiles, wind blown dust particles created a charging rate many times higher than that exhibited by conventional aircraft materials. This may have been due to the rough surface texture of the tiles. Preliminary data indicated the Shuttle will charge at eight times the rate of an exposed all metallic skinned airplane.

Separate measurements were made of surface and volume resistivity of the sample LI1500 tiles on hand. These data indicated much higher values than had been expected; in fact so high as to be unmeasureable ($\gtrsim 10^{12}$ ohms) by a 500 volt megohmmeter. This result, combined with the high charge rates observed, suggests a potentially severe P-static problem to both the TPS and avionics systems even under nominal entry conditions.

To get a grasp of the magnitude of static discharge energy which could result from an Orbiter covered with LI1500 (or LI900) flying through typical ice crystal cloud formations, the following elementary analysis is offered:

Consider one tile of RSI, 6 inches square (surface area of 1 face = .0230m^2. Since most P-static charging will be in Orbiter frontal areas where heat and therefore tile thickness is greater, assume a tile thickness of 3.5 inches or .09m including the felt Strain Isolation Pad (SIP). From high voltage punch through tests conducted on LI1500 RSI, assume 100 kv/inch required to punch through the thickness of the tile (about the same as for air). Flashover around the surface is another possibility and may likely occur at much lower voltages. The flashover voltage is very difficult to predict but it will be a function of tile coating, humidity, pressure and contamination. For calculation purposes, assume 100 kv as the lower limiting voltage for flashover vs 350 kv as the upper limit via punch through. The charge stored on the surface of the tiles will be calculated for both cases.

First, the capacitance of the tile is $C = \frac{E\,A}{d}$. Assume $E = E_o = 8.85 \times 10^{-12}$ joules/newton-m^2.

$$C = 8.85 \times 10^{-12} \times \frac{0.023}{.09} = 2.26 \times 10^{-12} \text{ farads}$$

since $Q = CV$,

the charge for flashover, $Qf = (2.26 \times 10^{-12})(10^5) = 2.26 \times 10^{-7}$ coulombs.

the charge for punch through, $QP = (2.26 \times 10^{-12})(3.5 \times 10^5) = 7.9 \times 10^{-7}$ coulombs.

The energy of one spark discharge from a capacitance of 2.26×10^{-12} farads can also be calculated:

$$E_f = \frac{1}{2} CV^2 = \frac{(2.26 \times 10^{-12})(10^5)^2}{2} = 1.13 \times 10^{-2} \text{ joules}$$

$$E_f = 113{,}000 \text{ ergs}$$

similarly $E_p = 1.38 \times 10^6$ ergs

These calculations indicate spark energies of hundreds of thousands of ergs are possible. From Paragraph 1.2 it has been shown that a spark energy as low as 565 ergs is sufficient to upset a computer logic in an actual spacecraft installation. Assuming a charging rate of 40 μamps/square foot as measured on conventional aircraft in flight, one tile would see a charge rate of 10 μamps (10^{-5} coulombs/second)resulting in 44.2 flashover discharges of 113,000 ergs per second per tile, or 12.7 punch through discharges of 1.3×10^6 ergs per second per tile.

Although the number of tiles representing the electrical equivalent of the Orbiter frontal area has not been calculated, it is reasonable and conservative to estimate 1000 tiles (250 sq. feet). Thus:

- o Total flashovers = 44,200/second at 113,000 ergs.
- o Total punch-throughs = 12,700/second at 1.3×10^6 ergs.
- o Equipment susceptibilities observed: one spark at 565 ergs.

APPENDIX II

DC-10 COMPUTER SYSTEM

The DC-10 uses four analog computer systems for flight control. The computer architecture is depicted in Figures 4 through 6. This system is, however, backed up by a mechanical cable flight control system. The four computers are grouped into two pairs to form a dual-dual computational system. That is, computer 1A outputs, of Figures 4 or 5, are compared with computer 1B outputs and computer 2A outputs are compared with computer 2B outputs. There are no cross comparison, between computers 1A/1B and 2A/2B. Comparisons are made four times in the computational path on actual commands. Sensor signal differences, for example, to computers 1A and 1B are subtracted out (equalized or cancelled) since the detection of short period variations between channels is of interest. These short period variations, rather than long term variations, between the computational channels are indicative of channel failure. Similarly, the computational difference between the two channels under comparison are subtracted out (cancelled out) so that the comparators will only sense true failures.

When a non compare is indicated between two computational channels both channels are switched out of the system because it cannot be determined which channel has failed. However, in some DC-10's a PAFAM unit is used in addition to the four computational strings. In this

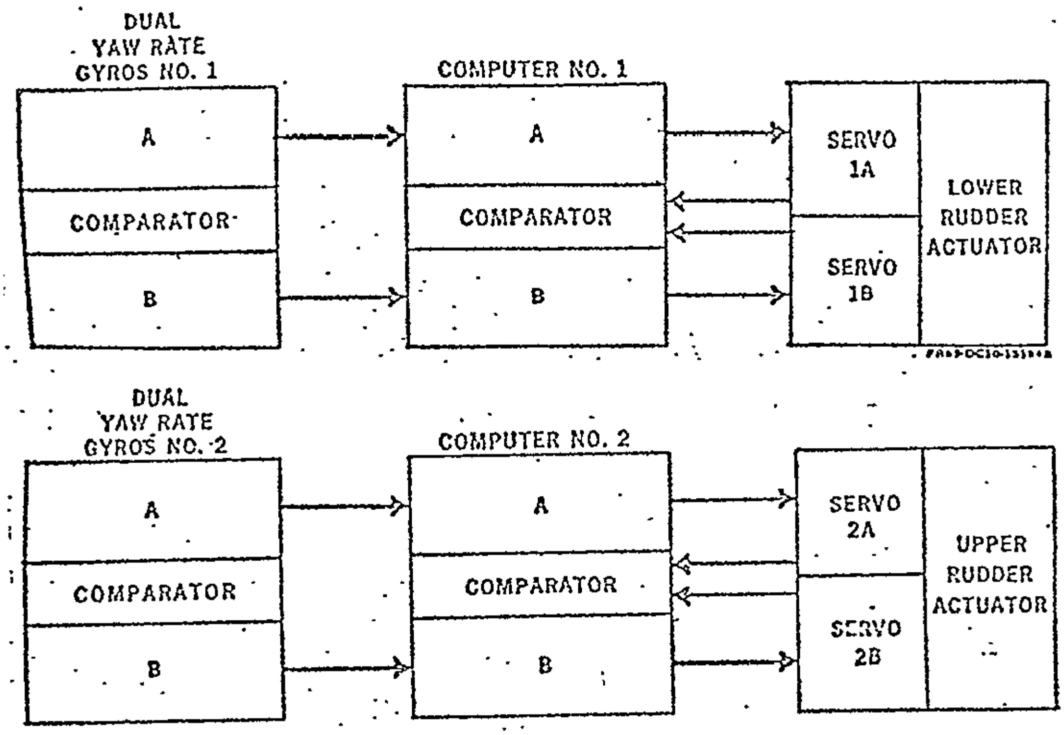


FIGURE 4 - TYPICAL DC-10-FOUR.CHANNEL SYSTEM

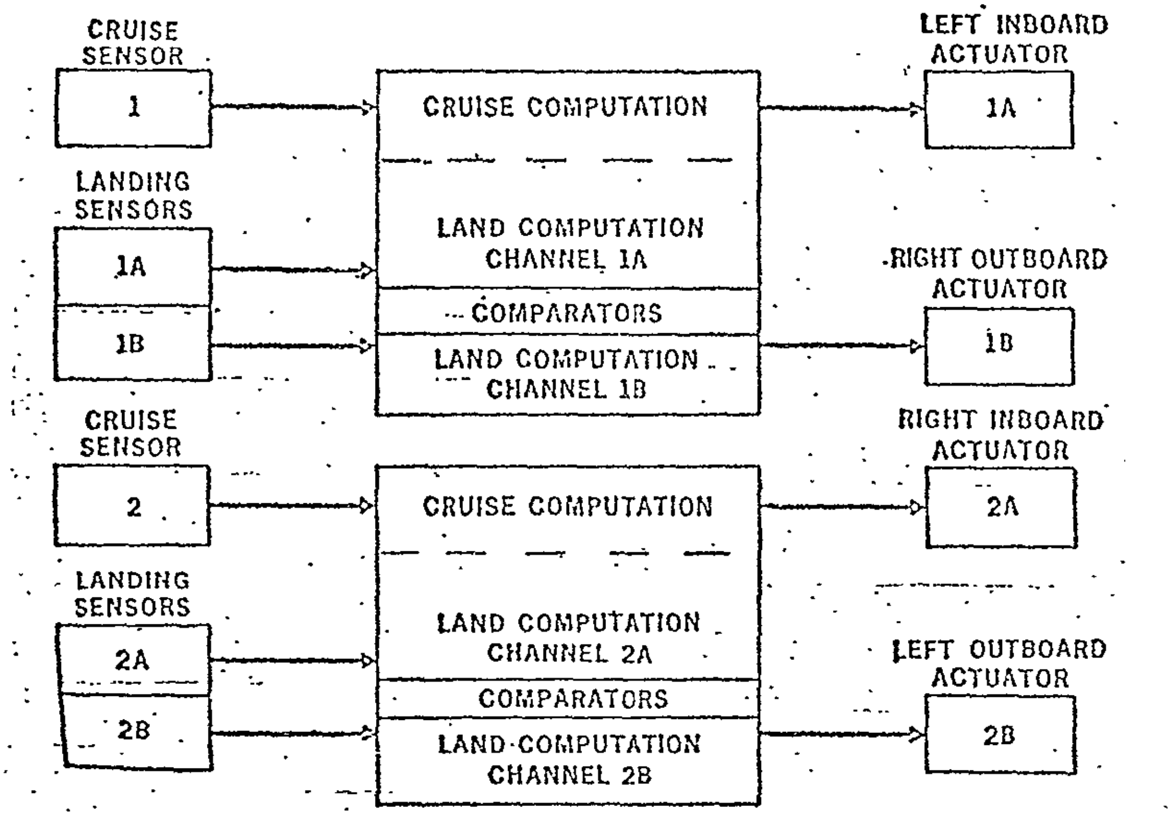


FIGURE 5 - DC-10 SIMPLIFIED AUTOMATIC PILOT BLOCK DIAGRAM

ORIGINAL PAGE IS
OF POOR QUALITY

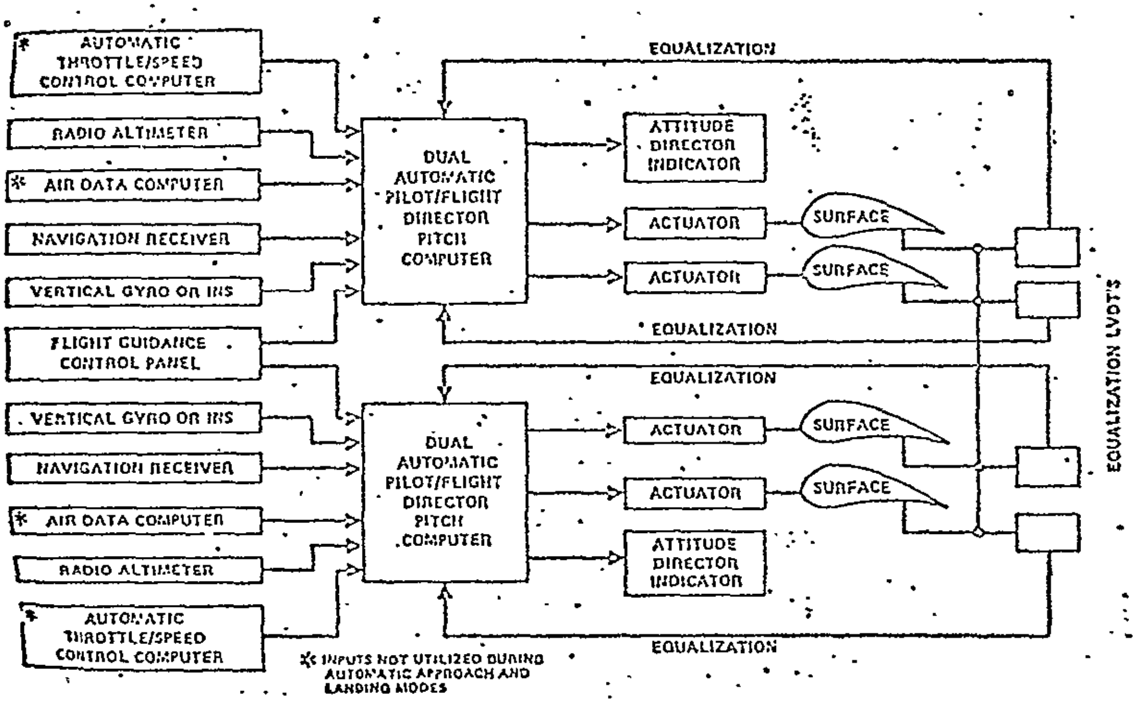

* AUTOMATIC THROTTLE/SPEED CONTROL COMPUTER
RADIO ALTIMETER
* AIR DATA COMPUTER
NAVIGATION RECEIVER
VERTICAL GYRO OR INS
FLIGHT GUIDANCE CONTROL PANEL
VERTICAL GYRO OR INS
NAVIGATION RECEIVER
* AIR DATA COMPUTER
RADIO ALTIMETER
* AUTOMATIC THROTTLE/SPEED CONTROL COMPUTER
DUAL AUTOMATIC PILOT/FLIGHT DIRECTOR PITCH COMPUTER
DUAL AUTOMATIC PILOT/FLIGHT DIRECTOR PITCH COMPUTER
ATTITUDE DIRECTOR INDICATOR
ACTUATOR
ACTUATOR
ACTUATOR
ACTUATOR
ATTITUDE DIRECTOR INDICATOR
SURFACE
SURFACE
SURFACE
SURFACE
EQUALIZATION
EQUALIZATION
EQUALIZATION
EQUALIZATION
EQUALIZATION LVDT'S
* INPUTS NOT UTILIZED DURING AUTOMATIC APPROACH AND LANDING MODES

FIGURE 6 - DC-10 AUTOMATIC FLIGHT CONTROL SYSTEM

ORIGINAL PAGE IS
OF POOR QUALITY

case the PAFAM can be used to determine which of the two strings has failed so that the good string can remain active. The PAFAM unit will prevent autoland systems disconnection if it observes no hardover failures and if it observes no performance degradation. This is true even if the comparators for the computational strings indicate a "non compare" or failed condition.

The PAFAM unit provides dissimilar functional redundancy to the flight control system. The unit is digital and is 100 percent self monitored and includes a watch dog timer, sample check, and check of proper register transfer. The unit is designed to meet FAA criteria of less than or equal to one false indication in 10^9 indications.

The PAFAM provides supervisory control of autoland disconnect functions, as noted previously. It includes a fast time model for prediction of the aircraft touchdown point. This predicted touchdown point is displayed to the crew. "Takeover" and other advisory commands are displayed to crew when a failure is detected by the PAFAM. The PAFAM notifies the crew of a failed condition and allows computer switching but doesn't accomplish switching by itself. The PAFAM also acts as a third entry for verification of failed computation strings. When two strings fail due to a non compare the PAFAM restores one computational string to use—the good one.

The DC-10 program has indicated that two types of system degradations must be designed for: equipment malfunctions and input source errors. Input source errors include wind sheers and erroneous landing system beams. With input signal source errors the comparators for the redundant computational path will indicate a compare condition but the vehicle may not be going to land on the runway. The PAFAM unit uses the fast time model to detect input source errors and to predict the touchdown point.

The PAFAM receives all inputs received by the other computational strings plus it uses other sensors such as accelerometers to accomplish its supervisory functions.

The PAFAM has been found useful but not mandatory for autoland. During development the PAFAM confirmed non-optimum control laws and assisted by indicating when manual takeover was required. The PAFAM was included in the initial system planning, because it was felt that something could be overlooked in automatic system design and at the time pilots had a low confidence level in autoland systems.

The DC-10 has an analog flight control system because at the time of development all industry experience was analog and there was a high confidence in the ability to control and suppress electromagnetic impulses in analog flight control systems. On the DC-10 program a trade was made between triplex and quad computational strings. Quad was selected due to its lower sensitivity to failures and because the quad approach matched plans for four control surfaces, and sensors in pairs.

APPENDIX III

L-1011 COMPUTER SYSTEM

The L-1011 uses four analog computer systems for flight control. The computer architecture is depicted in Figure 7. This system is, however, backed up by a mechanical cable flight control system. The four computers are grouped into two pairs to form a dual-dual computational system. Comparisons are made between the strings of each dual set in both the ILS and automatic flight control system. The voters select the best computer outputs. For example, one of two center signals are selected or the center signal is selected after one failure. For the command rate and command position servos the servo feedback to the servo amplifier must equal the servo amplifier command within a given tolerance. A false condition indicates a failure.

On this system two failures of a similar nature cause complete and automatic disconnection of the autopilot. The pitch and roll channels are not dual-dual in the autoland mode. The yaw channel is always dual-dual.

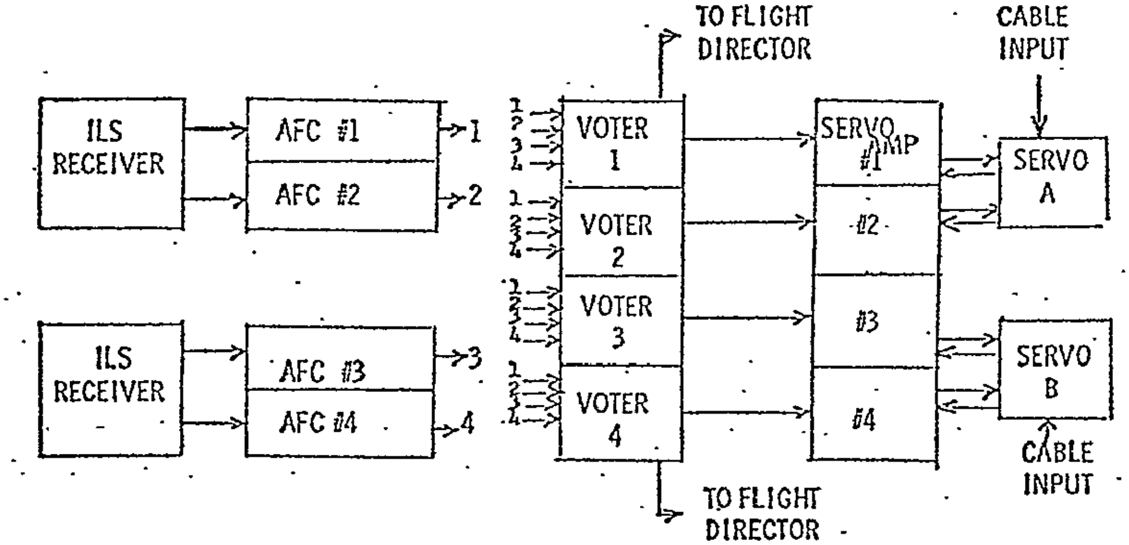


FIGURE 7 - L-1011 FLIGHT CONTROL SYSTEM

APPENDIX IV

B-1 COMPUTER SYSTEM

The B-1 uses four analog computational systems for flight control. The computer architecture is depicted in Figure 8. This system is, however, backed up by a mechanical cable flight control system. The four computers are grouped into two pairs to form a dual-dual computational system. Comparisons are made between the strings of each dual set in both the flight control electronics outputs and the actuators. Equalization of signals between two channels is accomplished at the actuators.

The requirement for operation is fail operational, fail safe. The failure reversion modes used are four computational strings active to two strings active to mechanical cable control. The mechanical system can fly the vehicle safely. The reason for functional redundancy—fly-by-wire and fly-by-cable is that this was a proven and safe design. The disconnection of the fly-by-wire system is both at the flight control output and the actuators shown in Figure 8. Disconnection is accomplished at the actuators if the system cannot compensate for differences in channels, within safe limits.

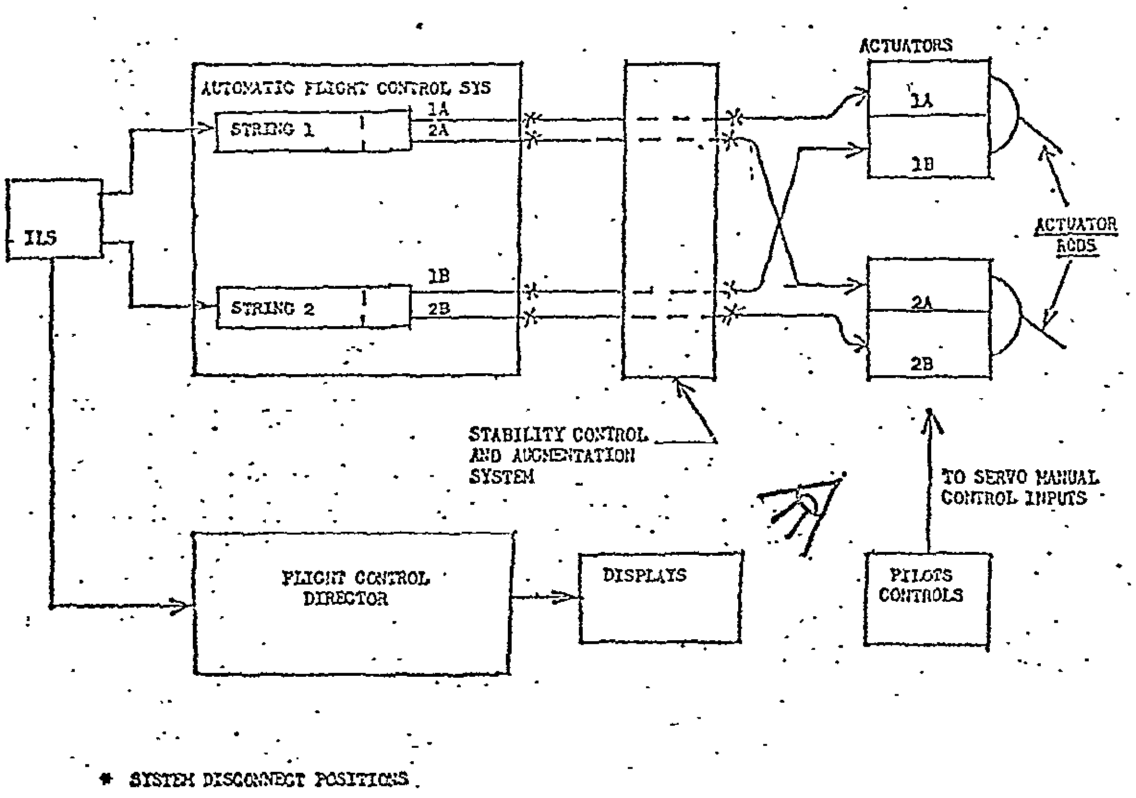


FIGURE 8 - B-1 FLIGHT CONTROL SYSTEM

ORIGINAL PAGE IS
OF POOR QUALITY

APPENDIX V

DC-10 DIGITAL R&D COMPUTER SYSTEM

This digital flight control system is a "dual, quad" system used for both flight control and autoland. The system consists of two digital computers driving four analog systems. The digital computers have digital to analog output channels and analog to digital conversion on the input channels. Each digital computer drives two analog strings. The analog strings have an output comparison logic which removes two strings at a time if a "no-compare" situation occurs. One digital computer and two analog strings work together as a dedicated system which is not cross strapped with the other digital computer and its two analog strings.

A single system consisting of one digital computer and two analog strings was installed in parallel with one-half of the normal DC-10 analog system and flown successfully several times. No DC-10 PAFAM system was used during these flights.

APPENDIX VI

F-4 COMPUTER SYSTEM

The F-4 autoland system uses a simplex autoland autopilot coupler system. Autoland commands for the system are generated by the SPN-42 radar tracking landing system which is located on aircraft carriers or on the ground. Commands from the SPN-42 are transmitted to the F-4 via an ASW-25 data link system. In addition to this autocoupler system a secondary landing system is located on the F-4. This secondary, SPN-41 (or C-SCAN), landing system is a microwave landing system that provides azimuth and elevation error information to the pilot similar to the conventional ILS. The SPN-41 is used by the pilots to ascertain that the SPN-42 autocoupler autoland system is functioning properly. The SPN-41 system is not an autoland system however, it provides a measure of functional redundancy since the SPN-41 may be used (weather permitting) to accomplish a manual landing if the SPN-42 autocoupler system fails. The primary function of the SPN-41 is to provide confidence to the pilots that the autoland system (SPN-42 coupler) is performing an accurate automatic landing.

Failure cues for the pilots are obtained in several ways. Failure are deduced from the secondary SPN-41 system displays, from manual or waveoff commands generated at the shipborne or ground terminal and transmitted to the F-4 via the data link, and from the master caution and coupler off light.

The criteria for deactivating the autoland coupler mode are: no commands received on board via the data link for "X" seconds, hardover control surfaces, and aircraft outside safe boundaries set by the ground. If any of these conditions are true the autocoupler system will automatically disconnect, requiring manual takeover. When the coupler and autopilot are disengaged from the autoland mode the systems are placed in the stability augmentation mode.

APPENDIX VII

F-8C COMPUTER SYSTEM

The F-8C fly-by-wire control system includes a digital primary system and an analog backup system. These systems were substituted for the normal F-8C mechanical flight control system. The Apollo computer was used as the heart of the primary system. As shown in Figure 9 a simplex digital primary systems and a triplex electrical analog backup system were used. As shown there was an active and a monitor servo path. If a failure occurred in either path a hydraulic comparator would sense the differential pressure between the active and the monitor servo valve and transfer control to the backup control system. As long as the primary control system was generating commands normally, the backup control system would track the active channel by way of the synchronization network. Only the hydraulic pressure was bypassed at the secondary actuator, so that the backup system was ready to take over at any time. If a transfer to the backup system was requested, the bypass was removed and the synchronization network was disabled, resulting in immediate proportional control from the pilot's stick. In the backup mode, the active servo valve was blocked and the secondary actuator operated as a force summer for the three backup channels. The digital computer continued to operate, computing the control laws which gave the best estimate of what the backup system commanded. If a transfer to the primary control system was attempted, the

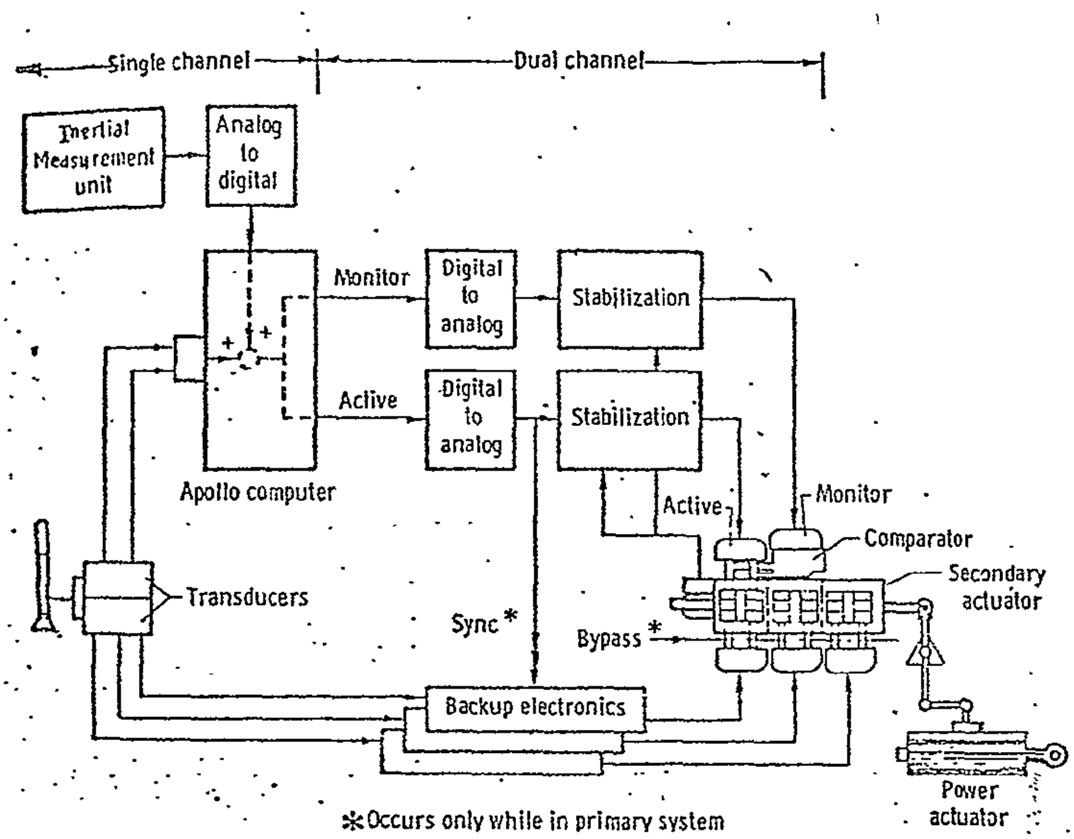


FIGURE 9 – F-8C DIGITAL FLY-BY-WIRE SYSTEM MECHANIZATION

transient was small as long as the computer was tracking the backup system. If the error was excessive between the primary control system and the backup control system, a cross-channel comparator prevented transfer to the primary control system.[1]

Since the trim inputs, sensor position inputs, and electronic gains were not necessarily the same in each backup control system channel, equalization was included to reduce errors between channels. Electronic and servo signals were monitored at two points within the backup control system. The channel voter output was compared with the channel voter inputs. If the difference was greater than the set threshold, the monitor was latched and the electronic channel was reported failed.[2]

Although built-in fault detection was extremely important for both the primary and the backup systems, it was of particular importance in the primary system. Because the primary system was full authority as well as single channel, its responses could have beeen hazardous if failures were not handled properly. Therefore, it had to be established that no digital computer system hardware failure would cause a hardover or otherwise hazardous signal. Figure 10 shows the type of digital system failure detection used. The Apollo computer had extensive and proven fault detection and reporting system which was built into the computer (item 1 in figure 10). This system, modified slightly for application to the F-8C airplane, was the most

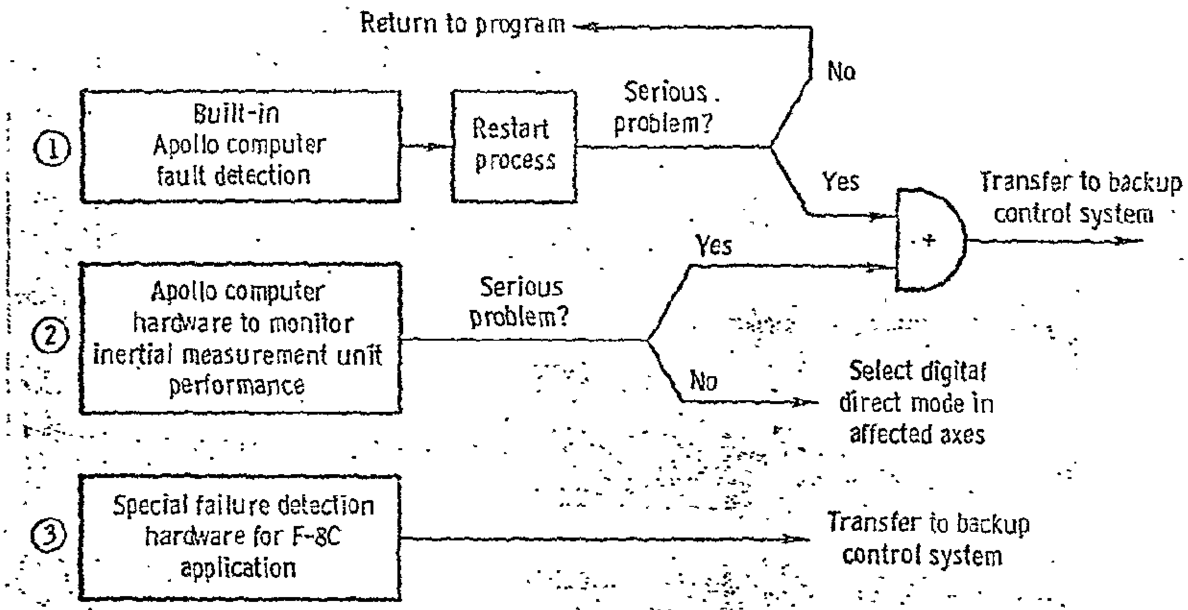

Return to program
No
Serious problem?
Yes
Transfer to backup control system
1
Built-in Apollo computer fault detection
Restart process
2
Apollo computer hardware to monitor inertial measurement unit performance
Serious problem?
Yes
No
Select digital direct mode in affected axes
3
Special failure detection hardware for F-8C application
Transfer to backup control system

FIGURE 10 – DIGITAL SYSTEM FAILURE DETECTION AND REPORTING SYSTEM

significant portion of the failure detection system. Some of the types of failures detected were:[1]

Logic circuits -

Parity failed

Program entered loop and did not exit

Program attempted to access unused read-only memory

Program failed to check in occasionally

Analog circuits -

Voltage went out of limits

Oscillator failed

Timing pulse generator failed

Each of these failures caused a restart, that is, a hardware-forced transfer out of control law program to a software routine which performed several clearing and initialization steps in attempt to correct the cause of the restart before allowing control law computations to continue. For some restart conditions, a signal was issued which caused a transfer to the backup control system.

The Apollo computer also monitored the performance of the inertial measurement unit (item 2, Figure 10). Written into the software were decisions either to transfer the system to the backup control system for serious failures or to select the direct mode in the primary system for situations such as an inertial measurement unit accelerometer failure, which would affect only certain augumented modes.

Analysis of primary system failures showed the need for additional hardware failure detection circuitry (item 3, Figure 10). The failure of certain channel outbits not monitored by the Apollo computer, in combination with normal pilot reactions could have led to hazardous situations. These conditions first became apparent in piloted, closed-loop simulations using the iron bird simulator. The necessary hardware modifications were made and implemented in the system to circumvent these failure conditions or to cause a transfer to the backup control system when prevention was not possible.

Built-in test equipment for the backup system and primary electronics was provided. This self-test equipment could be activated only during preflight tests.

Another type of logic function was the software reasonability test which was applied to each surface command before it was sent to the digital-to-analog converter. If the new command differed from the previous command by more than a predetermined amount, the affected axis would have transferred to the direct mode. This down mode philosophy was based on the assumption that a reasonability limit would be exceeded because of generic failures in the augmentation control laws rather than because of a hardware failure which would have affected the direct mode as well. It was assumed that a hardware failure would have been detected by the built-in Apollo computer fault detection logic.

Preflight testing was accomplished by an automatic self-test procedure that provided a pseudo end-to-end testing of the system. The self-test involved the introduction of a logic controlled stimulus and the disabling of circuit functions, and it used in-flight monitors to indicate the response. The use of the in-flight monitors as the self-test feedback elements served to check the channel signal paths and the operation of the in-flight monitors. This resulted in a "bang-bang" type of test with no indication of system degradation.

The F-8C fly-by-wire system experience with two dissimilar systems provides information applicable to future systems which are likely to have dissimilar redundancy. Most of the problems were concerned with the syncronization of the two systems. The goal for transfers from one system to another was to minimize transients caused by the transfer. In each instance, the system in control was tracked by the other system so that transients would be minimized. However, the primary system tracked the backup system by estimating the surface command of the backup system based on the pilot's control commands and trim inputs only. In transfers from the primary system to the backup system, the backup system tracked the output of the primary system. Although this eliminated the need to reconstruct the primary system signal propagation in the backup system, it did open the possibility for unusual initialization conditions when the transfer occurred during an abrupt maneuver. Another factor was that a transfer from the primary system to the backup system could have been initiated automatically as a result of a failure, thus the failure analysis had to consider all possible failures that could have resulted in a transfer. The timing of this transfer was critical in some instances when it could have coupled with the pilot's normal response to cause unacceptable conditions.

Many of the non compare conditions occurring in the secondary actuator differential pressure networks were caused by tracking errors between differential pressure signals, which caused the comparators to trip. The problems were caused by component tolerances and valve nulls and were predictable for certain control stick locations.

No digital system failures were experienced during flight; however, some flights were made using the backup mode in order to evaluate the backup. It is planned to continue the F-8C fly-by-wire program (phase II) using a fully redundant triplex system to verify concepts of concerns to the Space Shuttle Orbiter. Verification of redundancy management software for digital processing and sensor fault detection, and reduced generic failure probabilities should result due to this simulation.

A dissimilar backup system will also be used. The first F-8C fly-by-wire flights were made in 1972 with additional flights in Phase II planned for 1975 through 1977.

APPENDIX VIII

F-15 COMPUTER SYSTEM

The F-15 uses a simplex computer with two data buses for those functions not in the safety of flight loop. In addition a separate digital differential analyzer (DDA) is used with an inertial platform for navigation. In case of a failure of the DDA the simplex computer serves as a backup to the DDA. In this system the pilot makes the decision to deactivate a failed computer. A panel light alerts the crew of a failed condition. Deactivation of the failed computer refers to disconnection of the failed unit since the failed unit continues to operate.

APPENDIX IX

F-4 FLY-BY-WIRE SYSTEM[3]

The F-4 fly-by-wire system as previously tested has no automated flight modes and therefore was not investigated extensively for this report. However, this system uses quad redundant electronics channels from the control stick to the control surfaces and uses elaborate failure detection and reporting circuitry. The panel display lights indicate both the failed electronics and failed actuators in each axis and each electronic string. These lights are driven from the comparator outputs. Failed electronics and failed actuators can be independently deactivated. Deactivation is accomplished automatically upon indication of a non compare condition. The comparator scheme used is similar to that described in Appendix XV, Advanced Computer System.

APPENDIX X

F-14 COMPUTER SYSTEM

The F-14 uses three special purpose digital computers which operate in a sequential manner. Each computer is dedicated to selected mission phases which overlap during the switching period. One computer is used for the take-off, climb, descent, and landing. Another, the Central Air Data Computer (CADC), is used for general flight. The third, Central Data Processor (CDP), is used for prime mission objectives such as target tracking and fire control.

A manual fly-by-cable backup mode is provided. This mode is achieved by manually overriding the electronic system. Mission phase switching is normally done automatically. The computers are not redundant and do not serve as a backup to each other.

APPENDIX XI

F-111 COMPUTER SYSTEM

The F-111 uses triple redundant electronics with middle value selection. A mechanical cable control system is available as a backup system.

APPENDIX XII

S-3A COMPUTER SYSTEM

The cross strapping arrangement used in the Univac 1832 Computer System is shown in Figure 11. This diagram indicates the extensive cross strapping between modules to prevent a single failure in a string from making a serial interface section inoperative. Also shown is the configuration for triple memory redundancy in which each processor has independent access to all memory banks.[4]

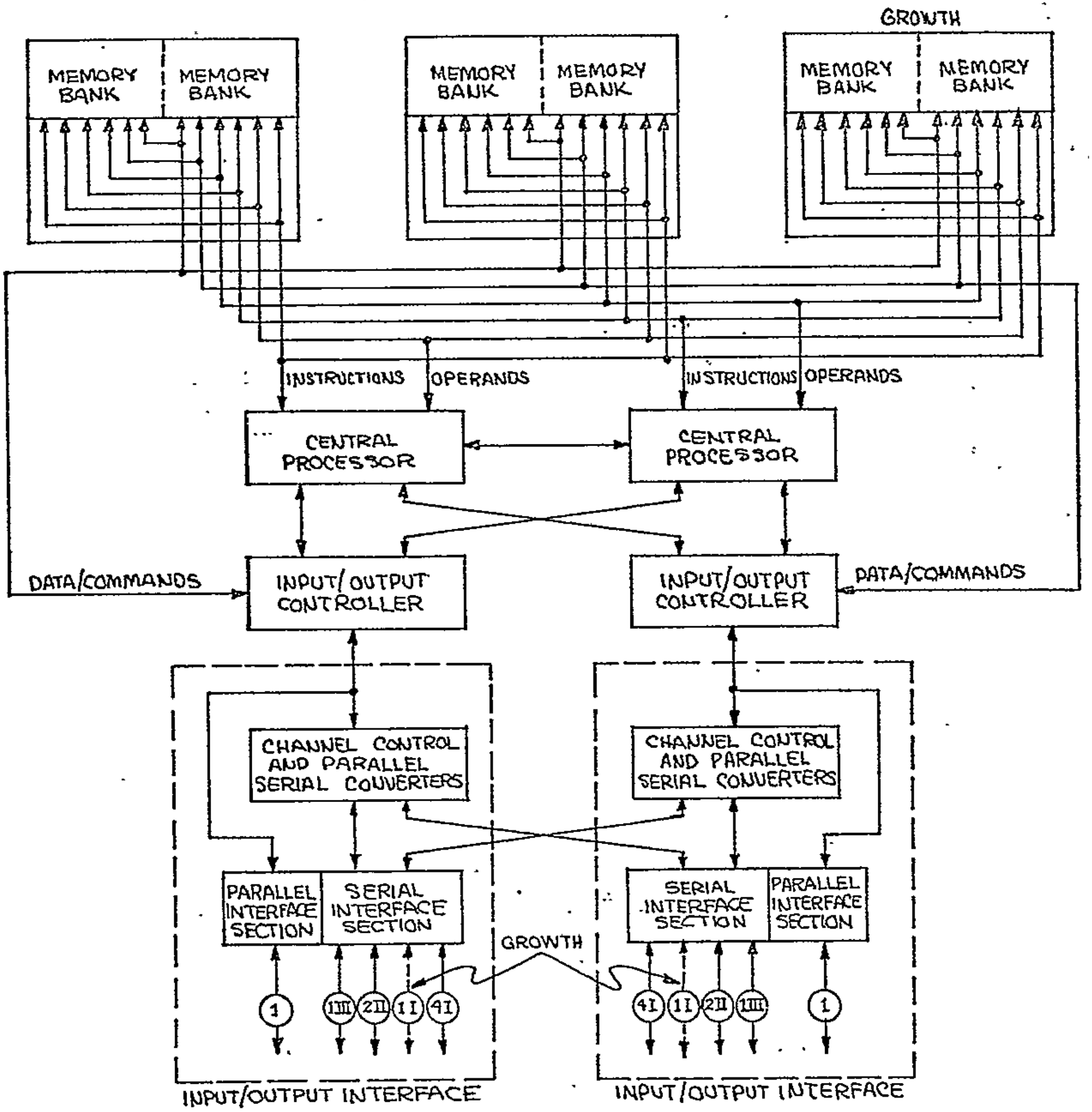


FIGURE 11 - S-3A DATA MANAGEMENT SUBSYSTEM

ORIGINAL PAGE IS
OF POOR QUALITY

APPENDIX XIII

TAGS COMPUTER SYSTEM[5]

The Tactical Aircraft Guidance System (TAGS) was designed to evaluate advanced flight control concepts for the CH-47 helicopter. The system consisted of a triple redundant flight control system. A simplified block diagram for TAGS is shown in Figure 12. As shown the triplex sensors are dedicated on a channel basis for data acquisition. The flight control actuator command selection circuits use middle value selection algorithms. The actuators are triplex and force-sharing through use of a mechanical force-summing bar. A more detailed system block diagram is shown in Figure 13.

TAGS did experience a psychotic type failure due to programming oversights. The program as initially designed could not handle a second failure in a second computer before three computation cycles had elapsed since the first failure. This resulted in a complete shutdown of all three computer systems due to a single failure. Reversion to a mechanical backup system was required to preclude loss of control.

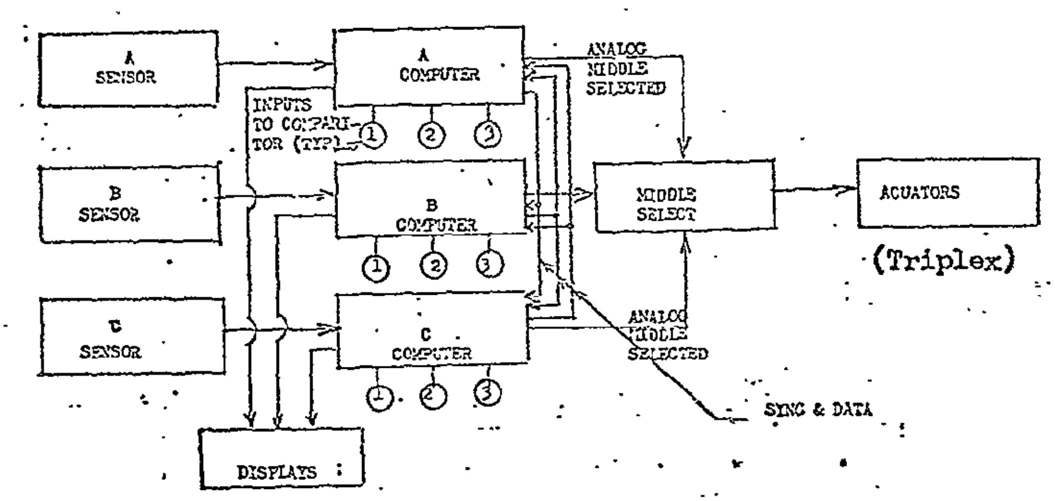


FIGURE 12 - TAGS FLIGHT CONTROL SYSTEM

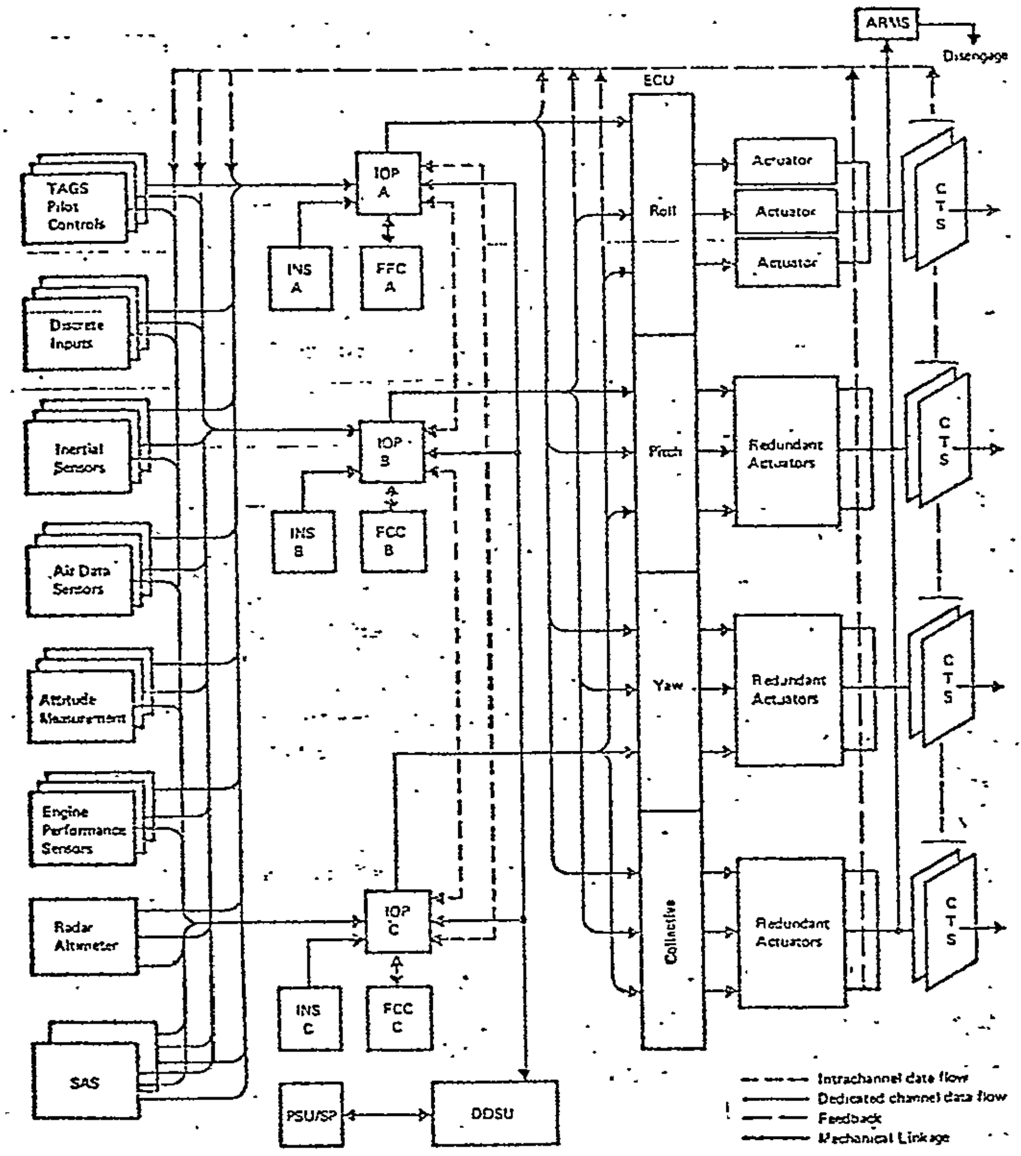


FIGURE 13 - TAGS CONFIGURATION BLOCK DIAGRAM

ORIGINAL PAGE IS
OF POOR QUALITY

YF-16 COMPUTER SYSTEM[6]

The YF-16 uses a quadruple redundant all fly-by-wire control system. The system has four independent computational paths and uses a middle signal select algorithm; except after two failures a lower signal select algorithm is used. No fly-by-cable system is retained in the YF-16. After the middle value is selected, the selected signal is quadrupled so that four identical signals are available as outputs to the servo actuators. Three outputs of the computational string, e.g. A, B, and C, as shown in Figure 14, are compared at one time. If one of these three strings, e.g. B, varies a predetermined amount from the other two, then string D is substituted instantaneously and automatically for B.

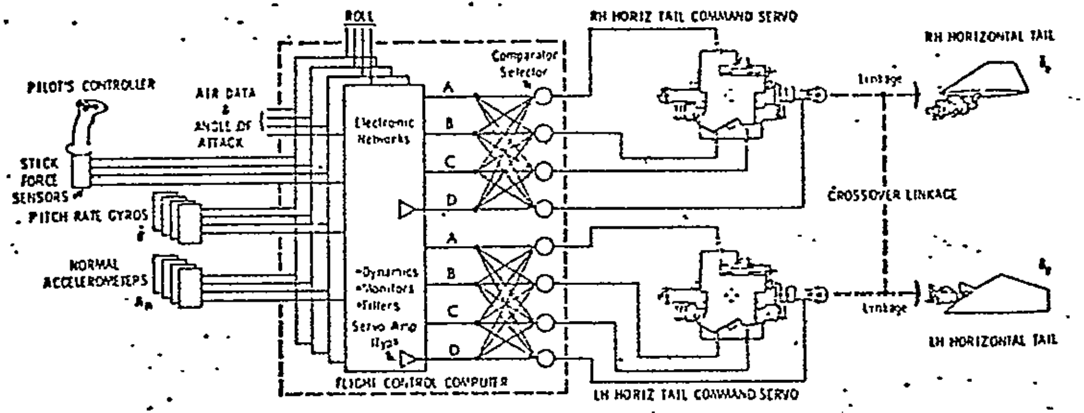


FIGURE 14 - YF-16 FLIGHT CONTROL SYSTEM

ORIGINAL PAGE IS
OF POOR QUALITY

APPENDIX XV

ADVANCED COMPUTER SYSTEM

An advanced flight control system that was under investigation for advanced fighter aircraft by McDonnell Douglas is depicted in Figure 15. This figure shows how two comparison points can be used in a computational and control electronic string. One at the output of the actuators so that complete strings are being compared and one at the output of computational circuits so that an actuator is not lost due to a computational fault. The voter (signal selector) is to be designed so that a failed input is never selected as the output of the voter. The comparators at the actuators measure pressure differential between actuator outputs in a manner such that the failed string can be detected. For example, if for comparator A input 1A1 does not compare with 1A2 and for comparator B input 1B1 does not compare with 1B2 a failure in string "one" is indicated. The same type of comparator arrangement would be used to detect failures in string two, three and four.

Four control strings are used so that fail operational, fail operational, fail safe (FO/FO/FS) operation can be achieved using only four comparators.

The voters can use standard selection algorithms such as select second from bottom value and middle value select.

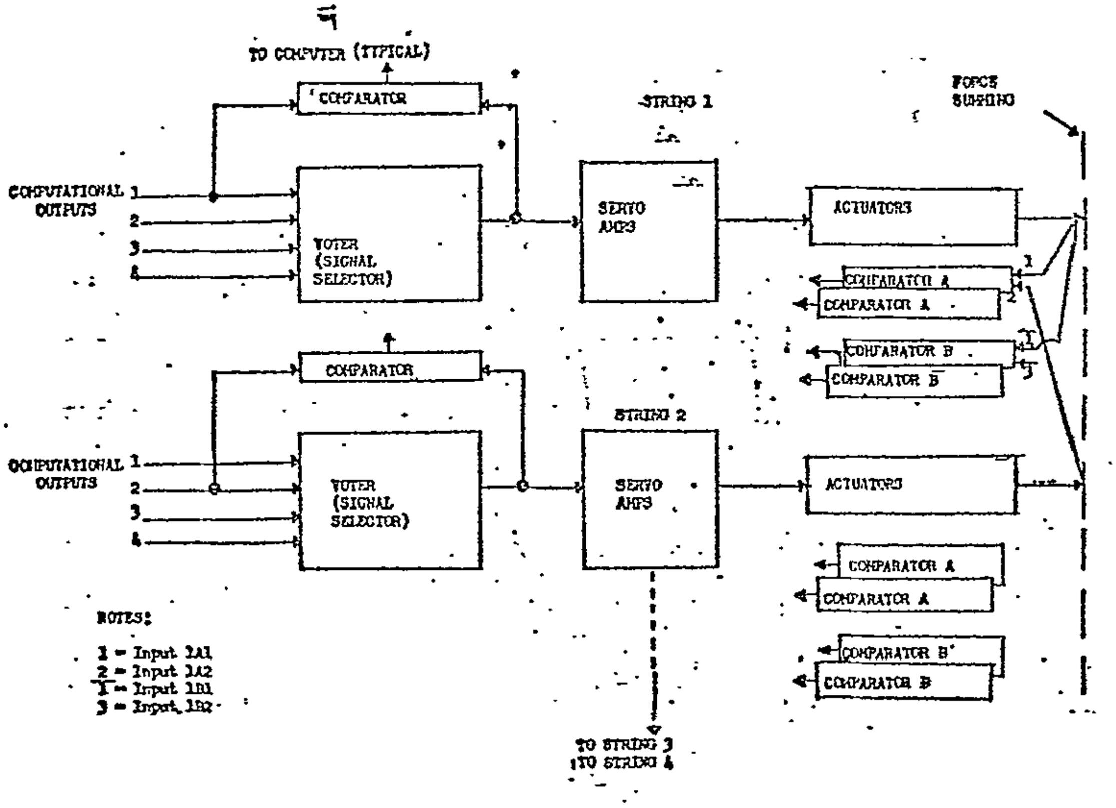


FIGURE 15 - ADVANCED STUDIES CANDIDATE SYSTEM USING QUAD COMPUTERS

APPENDIX XVI

SHUTTLE MAIN ENGINE COMPUTER SYSTEM

The current baseline consists of two digital computers residing in each main engine controller. One controller is dedicated to each of the main engines.

The redundant digital computers, for each main engine are both acquiring and processing data in parallel; however, they serve in a master and backup capacity. The output of the backup computer is not in an active control mode but serves on a standby capacity. A failure in the master will cause an automatic switchover to the backup computer. A second failure will cause the engine to shut down.

Since the two computers operate independently, except during the switching period, the implementation techniques do not appear to provide insight to the psychotic computer study problem area.

APPENDIX XVII

SATURN V INSTRUMENTATION UNIT COMPUTER SYSTEM?

The Saturn V Instrumentation Unit (IU) provides control to the three Saturn V booster stages. A single digital computer with duplex memory and triple modular redundancy is used. This system has no criteria to deactivate a failed computer. The failed computer would continue to operate and try to reinitialize. The crew is not involved in any manual reconfiguration procedures.

The Launch Vehicle Digital Computer (LVDC) shown in Figure 16 is a general purpose computer. The memory can be operated in either a simplex or duplex mode. In duplex operation memory modules are operated in pairs with the same data being stored in each module. Readout errors in one module are corrected by using data from its mate to restore the defective location. In simplex operation each module contains different data, which doubles the capacity of the memory. However, simplex operation decreases the reliability of the LVDC because the ability to correct readout errors is lost.

Computer reliability is increased within the logic sections by the use of triple modular redundancy. Within this redundancy scheme, three separate logic paths are voted upon to correct any errors which develop.

The Launch Vehicle Data Adapter/Launch Vehicle Digital Computer (LVDA/LVDC) receives the complement of the LVDA/LVDC

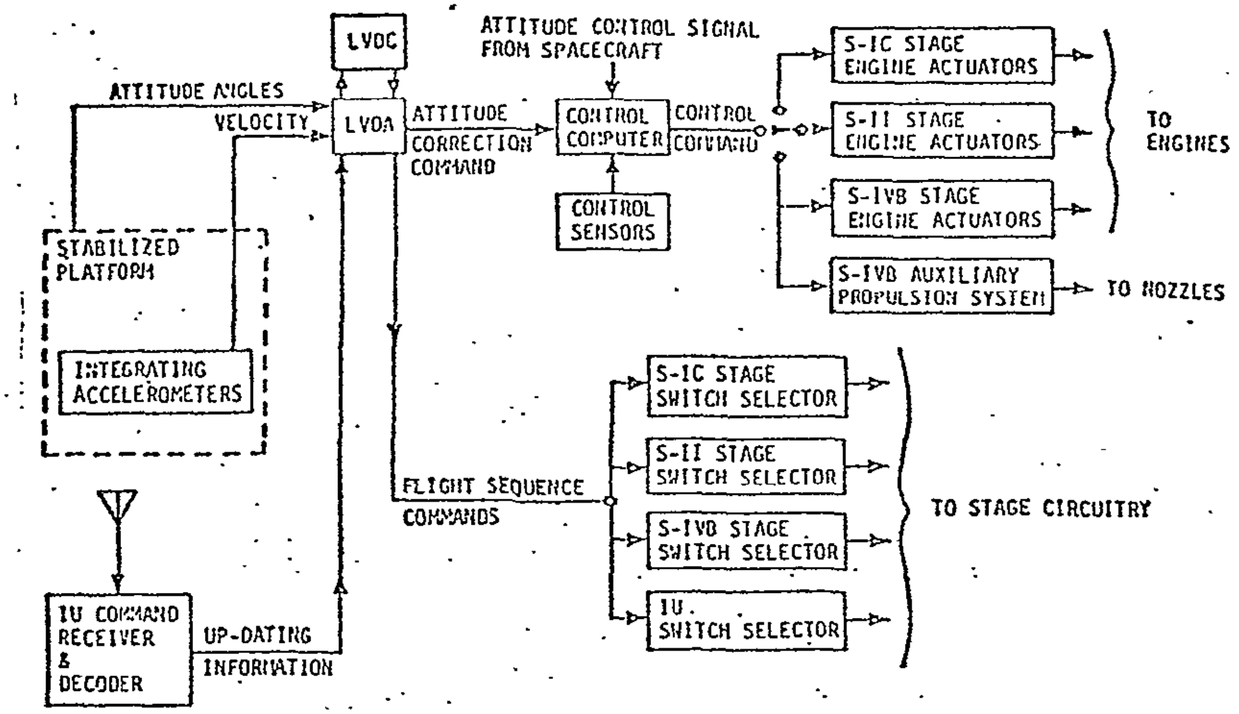

LVDC
ATTITUDE CONTROL SIGNAL FROM SPACECRAFT
ATTITUDE ANGLES
VELOCITY
LVDA
ATTITUDE CORRECTION COMMAND
CONTROL COMPUTER
CONTROL COMMAND
CONTROL SENSORS
S-IC STAGE ENGINE ACTUATORS
S-II STAGE ENGINE ACTUATORS
S-IVB STAGE ENGINE ACTUATORS
TO ENGINES
S-IVB AUXILIARY PROPULSION SYSTEM
TO NOZZLES
STABILIZED PLATFORM
INTEGRATING ACCELEROMETERS
FLIGHT SEQUENCE COMMANDS
S-IC STAGE SWITCH SELECTOR
S-II STAGE SWITCH SELECTOR
S-IVB STAGE SWITCH SELECTOR
IU SWITCH SELECTOR
TO STAGE CIRCUITRY
IU COMMAND RECEIVER & DECODER
UP-DATING INFORMATION

FIGURE 16 - INSTRUMENT UNIT NAVIGATION, GUIDANCE & CONTROL SYSTEM BLOCK DIAGRAM

ORIGINAL PAGE IS OF POOR QUALITY

command code after the flight sequence command (bits 1 through 8) has been picked up by the input relays of the switch selectors. This is indicated in Figure 17. The feedback (verification information) is returned to the LVDA, and compared with the original code in the LVDC. If the feedback agrees, the LVDC/LVDA sends a read command to the switch selector. If the verification is not correct, a reset command is given (forced reset), and the LVDC/LVDA reissues the 8-bit command in complement form, on the 8 parallel lines indicated.

The Saturn V uses a parallel data bus system as indicated in Figure 17.

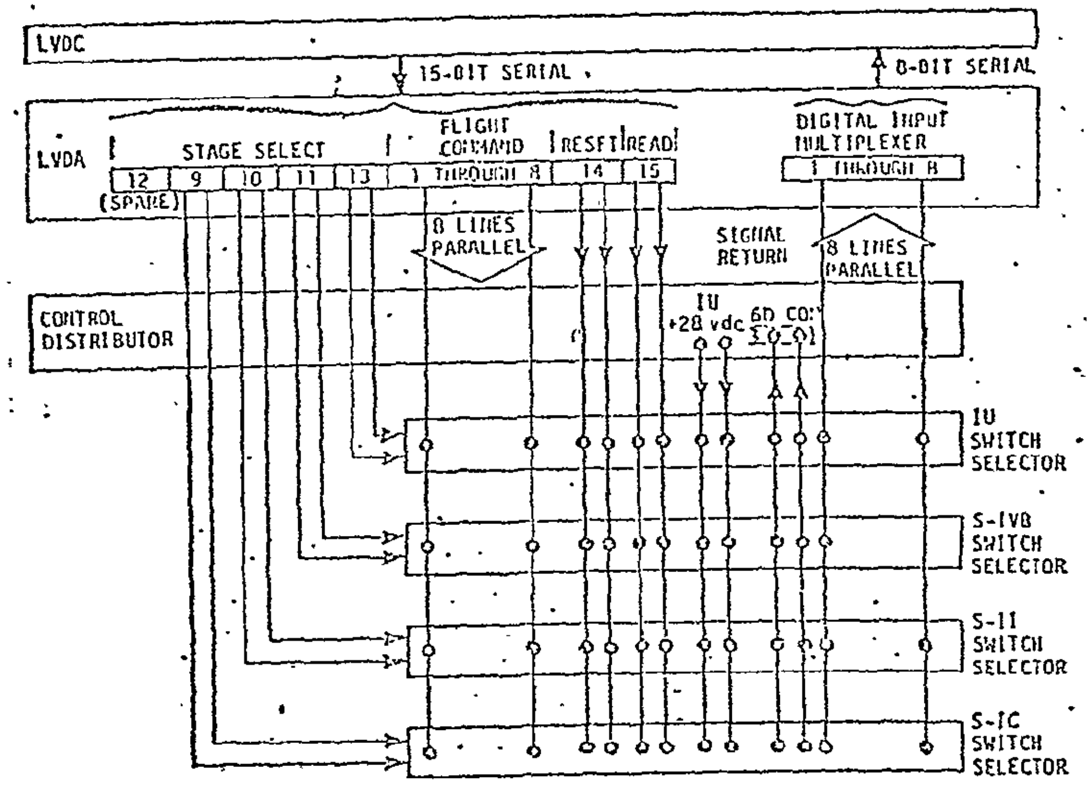


FIGURE 17 - INSTRUMENT UNIT LAUNCH VEHICLE DIGITAL COMPUTER (LVDC) SWITCH SELECTOR INTERCONNECTION DIAGRAM

APPENDIX XVIII

GROUND COMPUTER SYSTEMS

This appendix briefly defines the three ground computer systems investigated. These are the NASA JSC Mission Control Center (MCC), the NASA GSC remote site, and the NASA KSC Saturn Launch Vehicle (PAD 39) computer systems.

A. MCC Automated System

MCC - RTCC: five IBM 36-75 computers for processing

COATS: has four Univac 494 computers for interfacing with the Goddard network

- Two of each computer set is dedicated to a mission at the MCC
  - o Two computers are active during critical mission phases (launch, insertion, rendezvous)
    - o One is on-line; other is in dynamic standby mode
    - o Both get the same inputs, however the outputs of the standby are not used
    - o Computer status is determined by console operator
    - o Switching criteria is judgemental using procedures and console data
    - o Manual switching only, with no automatic capability available; msec timeframe (no data loss at MOCR consoles); break-before-make switchover
  - Computer/MOCR console interface is simplex data bus
- MCC/Goddard interface (COATS)
  - Redundant lines; one active, one not used
  - Backup line carries test messages to verify readiness

B. Remote Site Automated System

REMOTE SITES

- Two computers: One uplink (commands), one downlink (data or TM)
    - Dedicated by function, no redundancy
    - Realtime reconfiguration after failure, active computer does one function
    - Both computers can do either function but not simultaneously.
- Remote site/Goddard interface
    - One line
    - Realtime backup using alternate "MA BELL" lines

C. KSC Saturn Launch Vehicle (PAD 39) Automated System

- Two RCA 110A computers: 1 in LUT (Launch Umbilical Tower)
1 in LCC (Launch Control Center)
    - Not redundant
- Two LCC/LUT data buses: 1 active (in line)
1 passive
    - Passive line verification at system turn-on
    - Automatic switchover to the backup bus after two unsuccessful attempts to transfer data (does not switch back)
    - Hardline (3 miles) backup for critical functions