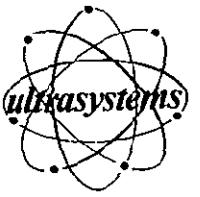
FINAL REPORT
ANALYSIS OF THE SURVIVABILITY OF THE SHUTTLE (ALT) FAULT-TOLERANT AVIONICS SYSTEM

APRIL 1976



ANALYSIS OF THE SURVIVABILITY OF THE SHUTTLE(ALT) FAULT-TOLERANT AVIONICS SYSTEM

FINAL REPORT

DATA REQUIREMENTS LIST ITEM 3

prepared for

Johnson Space Center
National Aeronautics and Space Administration
Houston, Texas 77058

Contract NAS9-14739

by

Ultrasystems, Inc.
2400 Michelson Drive
Irvine, California 92715

April 1976

76/6.43-9

FOREWORD

This document is submitted as the Final Report on the work performed under Contract NAS9-14739. The authors wish to acknowledge the technical direction and assistance provided by Mr. Allan E. Brandli and Mr. Curtis D. Warnick of NASA Johnson Space Center. They also wish to acknowledge the cooperation and assistance of Mr. Robert P. D'Evelyn of Rockwell International.

The Ultrasystems project manager was Mr. Ralph B. Conn. Other Ultrasystems contributors were Dr. Phil M. Merryman, Mr. Kim L. Whitelaw, Mr. Mark A. Wadsworth, and Mr. Richard H. Brock.

FINAL REPORT

TABLE OF CONTENTS

		PAGE
1.0	INTRODUCTION AND SUMMARY	1-1
	1.1 INTRODUCTION	1-1
	1.2 SUMMARY	1-3
2.0	BACKGROUND AND DESCRIPTION OF CAST	2-1
	2.1 BACKGROUND	2-1
	2.2 DESCRIPTION OF CAST	2-3
3.0	SHUTTLE (ALT) DATA PROCESSING SUBSYSTEM	3-1
4.0	ANALYTIC MODEL MODIFICATION	4-1
	4.1 SHUTTLE AVIONICS SYSTEM PARTITIONING	4-1
	4.1.1 GENERAL	4-1
	4.1.2 DETAILED PARTITIONING	4-3
	4.2 GPC MODELING	4-5
	4.2.1 STATE DIAGRAM DERIVATION	4-5
	4.2.2 FORMULATION AND SOLUTION OF EQUATIONS	4-7
	4.3 MCDS MODELING	4-9
	4.3.1 STATE DIAGRAM DERIVATION	4-9
	4.3.2 EQUATION DERIVATION	4-11
	4.4 FLIGHT CRITICAL BUS MODELS	4-15
	4.4.1 GENERAL	4-15
	4.4.2 DDU MODEL DERIVATION	4-17
	4.4.3 FLIGHT-CRITICAL-MDM SURVIVABILITY-MODEL DERIVATIONS	4-19
5.0	SIMULATOR	5-1
	5.1 SIMULATOR BACKGROUND AND MODIFICATIONS	5-1
	5.1.1 BACKGROUND - RCS SIMULATOR	5-1
	5.1.2 EXTENSION OF RCS WORK	5-3

TABLE OF CONTENTS (Cont'd)

PAGE

5.2 GENERAL DISCUSSION OF THE SIMULATOR 5-5

5.2.1 SIMULATOR CHARACTERISTICS 5-5

5.2.2 GLOBAL SIMULATOR ORGANIZATION 5-7

5.2.3 SIMULATOR UTILIZATION 5-9

5.3 SIMULATION OF THE GPCs 5-11

5.3.1 OVERALL GPC SIMULATOR STRUCTURE 5-11

5.3.2 STATE DIAGRAM 5-13

5.3.3 FAULT GENERATION 5-19

5.4 SIMULATION OF FLIGHT-CRITICAL BUS SUBSYSTEM 5-27

5.4.1 GLOBAL APPROACH TO FCB MODELING 5-27

5.4.2 FCB SUBSYSTEM STATUS REPRESENTATION 5-29

5.4.3 ORGANIZATION OF FCB SIMULATION PROGRAM 5-31

5.4.4 INTEGRATING FCB SIMULATION SUBROUTINES WITH THE MAIN PROGRAM 5-33

5.5 SIMULATOR UTILIZATION 5-35

5.5.1 SIMULATOR INPUTS 5-35

5.5.2 OBTAINING SIMULATOR INPUT PARAMETERS 5-39

5.5.3 INTERPRETATION OF SIMULATOR OUTPUT 5-43

6.0 DPS SURVIVABILITY ESTIMATES 6-1

6.1 BASELINE PARAMETER APPROACH 6-1

6.2 BASELINE RESULTS 6-3

6.3 SELECTED SYSTEM OPTIONS 6-33

6.3.1 USE OF ALTERNATE MDM PORT 6-33

6.3.2 TRANSIENT-FAULT RECOVERY OPTIONS 6-39

6.3.3 VARIATIONS IN THE DETECTABILITY PREDICTION 6-49

6.4 SUGGESTED IMPROVEMENTS 6-61

6.5 SYSTEM MODEL VERIFICATION 6-63

TABLE OF CONTENTS (Cont'd)

	PAGE
7.0 CONCLUSIONS AND RECOMMENDATIONS	7-1
7.1 CONCLUSIONS	7-1
7.2 RECOMMENDATIONS	7-3
REFERENCES	

LIST OF FIGURES

		PAGE
2.2-1	CAST ACTIVITY SEQUENCE AND INFORMATION FLOW	2-4
4.2-1	FAULT OCCURRENCE/RECOVERY STATUS STATE DIAGRAM	4-6
4.3-1	SYMBOLIC INTERCONNECTION DIAGRAM OF THE MCDS	4-10
4.3-2	FAULT OCCURRENCE/RECOVERY STATUS STATE DIAGRAM FOR THE MCDS	4-10
4.4-1	FLIGHT-CRITICAL BUS CONNECTIONS (ALT)	4-16
5.2-1	THE RCS SIMULATOR IS STRUCTURED TO PERMIT MULTIPLE RUNS .	5-6
5.2-2	PRINCIPLES OF A FAULT DRIVEN SIMULATION (BOX 3 OF FIGURE 4)	5-8
5.3-1	SIMULATOR STATE DIAGRAM	5-14
5.3-2	GENERAL ORGANIZATION OF THE FAULT GENERATOR	5-22
5.3-3	GENERATION OF THE OCCURRENCE OF THE FAULTS IN ONE MODULE (POISSON DISTRIBUTION)	5-26
5.4-1	FLIGHT-CRITICAL BUS CONNECTIONS (ALT)	5-28
5.4-2	STRUCTURE OF FCBFLT SUBROUTINE	5-32
5.4-3	FIFAU OVERALL CONTROL SEQUENCE	5-34
5.5-1	PARTITIONING THE AP-101 MEMORY	5-40
5.5-2	PARTITIONING OF THE AP-101 MEMORY STORAGE-PAGE	5-42
5.5-3	Y-DRIVER ANALYSIS	5-42
5.5-4	CONFIGURATION SUMMARY - PART 1	5-44
5.5-5	CONFIGURATION SUMMARY - PART 2	5-47
5.5-6	CONFIGURATION SUMMARY - PART 3	5-48
5.5-7	CONFIGURATION SUMMARY - PART 4	5-50
5.5-8	SIMULATOR STATISTICS	5-52
5.5-9	FLIGHT CRITICAL BUS STATISTICS	5-54
6.1-1	BASELINE PARAMETER VALUES	6-2
6.3-1	FAILURE PROBABILITY RESULTS FOR VARIOUS TRANSIENT RECOVERY OPTIONS AND TRANSIENT FAULT RATES	6-40

LIST OF TABLES

		PAGE
1.1-I	CONTRACT CONCLUSIONS	1-2
3.0-I	FAULT DETECTION, LOCATION AND RECOVERY ACTIONS	3-4
4.2-I	PARAMETER DEFINITIONS	4-8
4.3-I	SYMBOL DEFINITIONS	4-12
5.4-I	BUS - BTU INTERCONNECTION MATRIX	5-30
5.4-II	MDM - DEVICE INTERCONNECTION MATRIX	5-30
5.5-I	REQUIRED SIMULATOR INPUTS - GPC PARTITION	5-36
5.5-II	REQUIRED SIMULATOR INPUTS - FCB PARTITION	5-38
6.3-I	LEAKAGE RESULTS FOR TRANSIENT RECOVERY OPTIONS	6-40
6.3-II	VARIATIONS IN TRANSIENT FAULT RATE FOR THE DELAY RECOVERY TRANSIENT RECOVERY METHOD	6-41
6.3-III	VARIATIONS IN TRANSIENT FAULT RATE FOR THE DELAY RECOVERY TRANSIENT RECOVERY METHOD	6-42
6.3-IV	VARIATIONS IN TRANSIENT FAULT RATE FOR THE ROLLAHEAD RECOVERY METHOD	6-43
6.3-V	VARIATIONS IN TRANSIENT FAULT RATE FOR THE ROLLAHEAD RECOVERY METHOD	6-44
6.3-VI	VARIATIONS IN TRANSIENT FAULT RATE WITH THE MEMORY COPY RECOVERY METHOD	6-45
6.3-VII	VARIATIONS IN TRANSIENT FAULT RATE WITH THE MEMORY COPY RECOVERY METHOD	6-46
6.3-VIII	VARIATIONS IN TRANSIENT FAULT RATE WITH THE ROLLBACK RECOVERY METHOD	6-47
6.3-IX	VARIATIONS IN TRANSIENT FAULT RATE WITH THE ROLLBACK RECOVERY METHOD	6-48
6.3-X	FAILURE PROBABILITIES FOR IMPERFECT GPC DETECTABILITY	6-50
6.3-XI	FAILURE PROBABILITIES FOR IMPROVEMENTS IN DETECTABILITY FOR ALL DEVICES	6-50
6.3-XII	SIX HOUR SURVIVABILITY FOR INCREASES IN TACAN DETECTABILITY	6-51
6.3-XIII	SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 999 999	6-52

LIST OF TABLES (Cont'd)

		PAGE
6.3-XIV	SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 999 9	6-53
6.3-XV	SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 99	6-54
6.3-XVI	SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999	6-55
6.3-XVII	SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 9	6-56
6.3-XVIII	SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 99	6-57
6.3-XIX	SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 999	6-58
6.3-XX	SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 999 9	6-59
7.1-I	CONCLUSIONS	7-2
7.2-I	ALT-OFT DIFFERENCES	7-4

DEFINITIONS

A/D	Analog to Digital
ADC	Analog-to-Digital Converter
ADI	Attitude Director Indicator
ADS	Air Data System
ADTA	Air Data Transducer Assembly
AGE	Air/Ground Equipment
AIU	Avionics Interface Unit
ALT	Approach and Landing Test
AMEC	Aft Master Events Controller
AMI	Alpha/Mach Indicator
ASA	Aerosurface Servo Amplifier Assembly
AVVI	Altitude Vertical Velocity Indicator
BCE	Bus Control Element
BITE	Built-In Test Equipment
BTU	Bus Terminal Unit
CD	Commander Decoder MDM
C_N	$u_N v_N w_N$ Coverage (Probability System Recovers Given Fault Occurs)
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSE	Computer Support Equipment
D	Discrete
D/A	Digital to Analog
DB	Data Bus
DBI	Data Bus Interface Unit - Launch
DBN	Data Bus Network
DC	Display Coupler
DD	Decoder Driver

DDU	Display Driver Unit
DEU	Display Electronics Unit
DMA	Direct Memory Access
DPS	Data Processing Subsystem
DSKY	Display and Keyboard
DU	Display Unit
EIU	Engine Interface Unit
FCOS	Flight Computer Operating System
FDA	Fault Detection Annunciation
FDI	Fault Detection and Identification
FDIR	Fault Detection Identification and Recovery
FI	Fault Identification
FKB	Flight Display Keyboard
G&C	Guidance and Control
G&N	Guidance and Navigation
GN&C	Guidance, Navigation and Control
GPC	General Purpose Computer
GSE	Ground Support Equipment
HSI	Horizontal Situation Indicator
ICC	Intercomputer Channel
IDPS	Interface Digital Processor
IMU	Inertial Measurement Unit
INTRPT	Interrupt
I/O	Input/Output
IOP	Input/Output Processor
IOM	Input/Output Module
IPL	Initial Program Load

IRIG B	Inter-Range Instrumentation Group B
IU	Interface Unit
KBPS	Kilobits Per Second
KBU	Keyboard Unit
KB	Keyboard
ℓ_N	Transient Leakage (Probability of Failure of Transient Recovery Given Fault is Transient)
LRU	Line Replacement Unit
MCDS	Multifunction CRT Display System
MCIU	Manipulator Controller Interface Unit
MDM	Multiplexer/Demultiplexer
MEC	Master Events Controller
MIA	Multiplexer Interface Adapter
MM	Mass Memory
MMU	Mass Memory Unit
MSBLS	Microwave Scan Beam Landing System
MSC	Master Sequence Controller
MSU	Mass Storage Unit
MTC	Master Thrust Controller
MTS	Magnetic Tape System
MTU	Master Timing Unit
MUX	Multiplex
NASA	National Aeronautics and Space Administration
OFT	Orbital Flight Test
PCM	Pulse Code Modulation
PCMMU	Pulse Code Modulation Master Unit
PMAD	Performance Monitor Annunciator Driver
PMS	Performance Monitoring System
PROM	Programmable Read Only Memory

RA	Radar Altimeter
RAM	Random Access Memory
RCS	Reaction Control System
R_{DDU}	$e^{-\sigma_{DDU}T}$
RG	Rate Gyro
RGA	Rate Gyro Assembly
RHC	Rotational Hand Controller
RM	Redundancy Management
R_{M1}	$e^{-\sigma_{M1}T}$; M1 denotes MDMs 1 through 3
R_{M4}	$e^{-\sigma_{M4}T}$; M4 refers to MDM 4
RMC	Redundancy Management Control
ROM	Read Only Memory
RPTA	Rudder Pedal Transducer Assembly
S(T)	Survivability (Probability Hardware and Software Survives Over a Mission of Length T)
$S_A^{(k)}$	Unit A Survivability with Initial Redundancy Level k
SBTC	Speedbrake Thrust Controller
SCU	Sequence Control Unit
SIM	Simulation
SM	System Management
$S_{mn}(t)$	$\exp[-(m\ \delta_{km} + n\ \delta_{dn})t]$
SPI	Surface Position Indicator
SVC	Supervisor Call
TACAN	Tactical Air Navigation
TAEM	Terminal Area Energy Management
TBD	To Be Determined

TLM	Telemetry
TVC	Thrust Vector Control
TVCD	Thrust Vector Control Driver
u_N	Detectability (Probability Fault is Detected Given Fault Occurs)
v_N	Diagnosability (Probability Fault is Properly Isolated Given Fault is Detected)
w_N	Recoverability (Probability System Recovers Given Fault is Properly Isolated)
δ_N	$u_N\sigma_N + (1-u_N)\sigma_t$ Rate of Faults Resulting in Failure or Redundancy Degradation
λ	Permanent Fault Rate
σ_N	$\lambda + \ell_N\tau$ Permanent and Leaky Transient Rate
σ_t	$\lambda + \tau$ Total Fault Rate
τ	Transient Fault Rate

1.0 INTRODUCTION AND SUMMARY

1.1 INTRODUCTION

OBJECTIVE

The objective of the work reported here was to provide an extension of the Complementary-Analytic-Simulative Technique (CAST) so that it would be applicable to the Shuttle Data Processing Subsystem (DPS). The accomplishment of this objective is to be achieved using a two-step process. The first step is to provide models, both analytic and simulative, for analysis of the Approach-Landing Test (ALT) configuration. This document contains a report of this ALT modeling and analysis. Since CAST had already been shown to be applicable to multicomputer systems (NASA Report CR-132552), the emphasis during this work was placed on extending the CAST concept so it is applicable to computer systems including the multiplicity of input and output devices found in a real-time control system application. The modeling and analysis of the Orbiter-Flight Test (OFT) is yet to be undertaken.

ACCOMPLISHMENTS

The accomplishments of Contract NAS9-14739 are described below and are summarized in tabular form in Table 1.1-I.

The DPS mission-critical survivability for a six-hour mission was determined to be 0.999863 for the Shuttle ALT baseline configuration. Thus it can be said that for ALT, the survivability is adequate. However, the fact that orbiting missions of up to 30 days are planned illustrates the necessity of extending the ALT work to be applicable to OFT and actual mission scenarios.

The above analysis led to the evaluation of three selected options which identified two areas of possible improvement. These improvements would result from use of a recovery technique which combines rollahead with memory copy, and increased TACAN fault detectability.

The above analysis and resulting conclusions was made possible by: extending the GPC analytic model to include imperfect detectability; creating a new analytic model to handle configurations involving non-symmetrical interconnections (e.g. MCDS); creating a new analytic model to handle combinations of dependent device sets (e.g. flight-critical bus and connected units);

modifying the existing RCS simulator routines to achieve UNIVAC 1108 compatibility, and adding three routines to reflect transient recovery procedure differences; and developing a simulation, consisting of 29 routines, for the flight-critical-bus partition.

TABLE 1.1-I CONTRACT CONCLUSIONS

1. CAST Extended Successfully to DPS ALT (Step I---This Contract)
2. DPS ALT Mission-Critical Survivability Determined to be adequate, i.e., 0.999863 (Step I---This Contract)
3. OFT/Mission Survivability Unknown and much more Important to NASA
    - Mission
    - Mission Duration
    - System Complexity
4. OFT/Mission Survivability can be Determined Through an Extension of the ALT Models and Subsequent Analysis
5. Areas of Possible Improvement Determined to Date are:
    - GPC Transient-Recovery Procedure
    - TACAN Detectability

1.2 SUMMARY

The results reported here were obtained by use of the enhanced version of the complementary-analytic simulative technique (CAST) developed on this contract for application to the Shuttle (ALT) avionics system configuration. These enhancements include modification of the previous analytic and simulation models and development of new models for the configurations not considered in previous work. The results are based on a six-hour mission and failure rates obtained from, or authorized by, the NASA Project Monitor.

Figure 1.2-1 presents a summary of the Shuttle avionics DPS failure probabilities as a function of mission time for the baseline configuration. The curves behave as expected in one respect, i.e., the failure probability increases with time. However, it is seen that the GPC failure probability has climbed to very close to that of the MCDS, and will for longer mission times approach the failure probabilities of the other units, e.g., flight displays. This is explained by the fact that the GPCs have high fault detectability and redundancy, but a high failure rate. The good detectability and redundancy keeps the curve low for short missions, but the high failure rate ultimately takes over and drives the curve up. The curves illustrate the necessity to perform this type of analysis for OFT and mission scenarios.

Using CAST, the efficacy of each of three system options was investigated. It was found that use of the alternate MDM port for reconfiguration of GPC bus assignments will become useful during critical mission phases, when TACAN and/or microwave scan beam landing system units with lower failure rates become available. The use of a recovery technique consisting of rollahead combined with memory copy has the potential of reducing transient leakage to zero (i.e., no transient faults are mistaken for permanents). This compares with the result of 70.3% when using the baseline technique of delay recovery. This more sophisticated GPC transient-fault recovery technique is most useful in hostile transient-fault environments, or when GPC coverage is degraded. Improvement in TACAN detectability offers the most promise of improving the overall avionics failure probability. For example, improving the TACAN detectability from 0.999 to 0.9999, will decrease the overall avionics failure probability from $7.7(10)^{-5}$ to $5.6(10)^{-5}$.

Consideration was given to use of laboratory tests to verify the CAST models. Laboratory testing to verify the models presented here was found to be feasible, but the testing must be carefully designed so as to obtain the

maximum results in a reasonable test time. This test design, when performed, must include both the test procedure and the test implementation, e.g., computer programs for automatic fault injection.

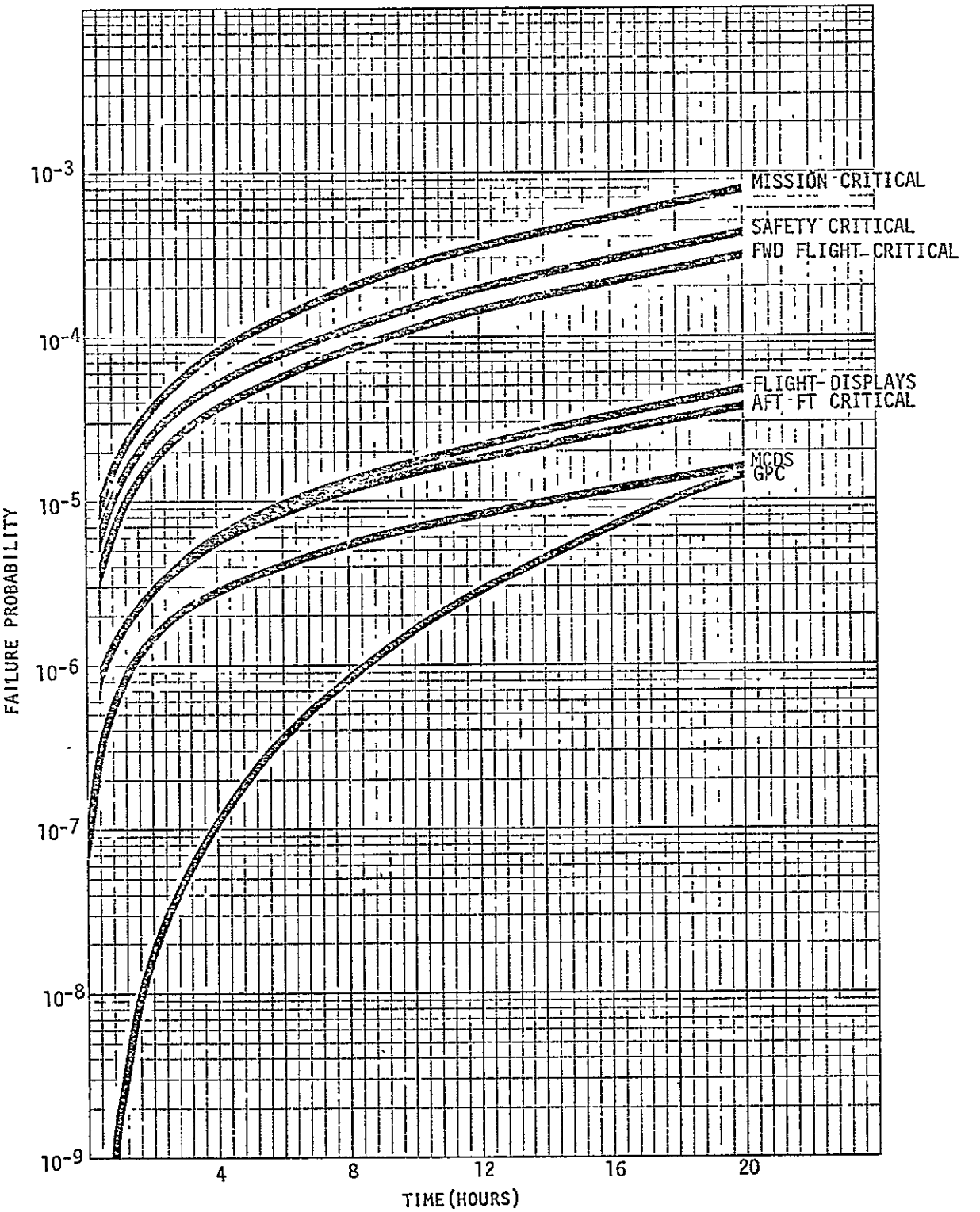


FIGURE 1.2-1 BASELINE CONFIGURATION FAILURE PROBABILITIES

2.0 BACKGROUND AND DESCRIPTION OF CAST

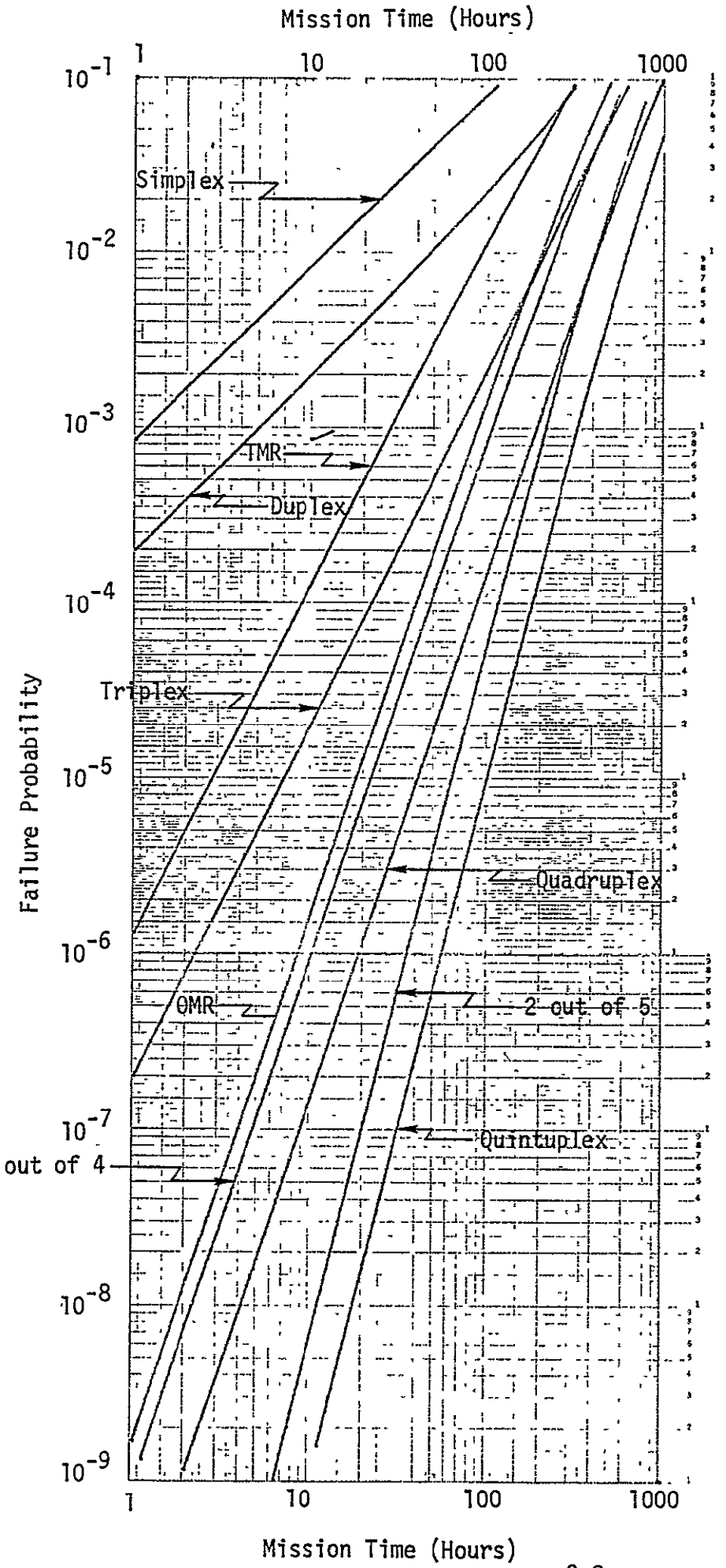
2.1 BACKGROUND

A complementary analytic-simulative technique suitable for extension to Shuttle applications was evolved on a previous contract.

The complementary analytic-simulative technique (CAST) evolved as a result of a study performed for NASA Langley Research Center. The objective of the study was to provide concepts and engineering data from which a highly-reliable, fault-tolerant, reconfigurable computer system (RCS) for aircraft applications could be designed. For the purposes of the study, an RCS was defined to be a redundant configuration of off-the-shelf avionics computers which achieved fault-tolerance through use of a variety of recovery techniques. A principal study goal was the development and application of reliability and fault-tolerance assessment techniques. Particular emphasis was placed on the needs of an all-digital, fly-by-wire control system appropriate for a passenger-carrying airplane.

As mentioned above, a complementary analytic-simulative technique (CAST) for calculation of predicted failure probabilities of multicomputer systems was evolved. In addition, measures of fault-tolerance applicable to general fault-tolerant computer systems were defined. CAST was applied to 39 example computer system configurations to provide insight into the important aspects of these configurations, as well as demonstrate the efficacy of the approach. Also, a set of customer-provided reliability-enhancement techniques (RETs) was expanded and their individual effectiveness was evaluated.

A representative set of results obtained from applying CAST to an RCS is shown on the opposite page.



REPRODUCIBILITY OF THE ORIGINAL PAGE IS POOR

EFFECTS OF RCS REDUNDANCY AND ADAPTABILITY ON FAILURE PROBABILITY

2.2 DESCRIPTION OF CAST

Fault tolerance measures can be produced through a combination of engineering characterization of the system, simulation, and analytic modeling.

Analytic modeling and simulation each has its strengths and limitations. However, when these two system evaluation approaches are combined are supplemented by an engineering characterization of the system, a very powerful technique results. The combination is illustrated in Figure 2.2-1.

This Complementary Analytic-Simulative Technique (CAST) evolved as it became evident that neither analysis nor simulation alone could satisfy all the RCS evaluation requirements. Analytic modeling provides flexibility and rapid, economical data generation. However, the solutions for some configurations are very cumbersome and, in certain cases, the mathematical model formulated is intractable. Simulation permits computer system details to be included easily, but data generation is slow and expensive. CAST permits the user to obtain the best features of both analytic modeling and simulation.

The engineering characterization is performed to provide six categories of information to the analytic modeling and the simulation. These information categories are: (1) configuration particulars, (2) fault environment, (3) system failure criteria, (4) software structure, (5) recovery features, and (6) test features. The individual items in these six categories are shown in the figure.

The following items are available as simulator outputs: (1) permanent-fault coverage, (2) transient-fault coverage, (3) detectability, (4) diagnostability, and (5) recoverability.

The analytic modeling provides the following measures of fault tolerance: (1) computer system survivability (or failure probability), and (2) computer system reliability.

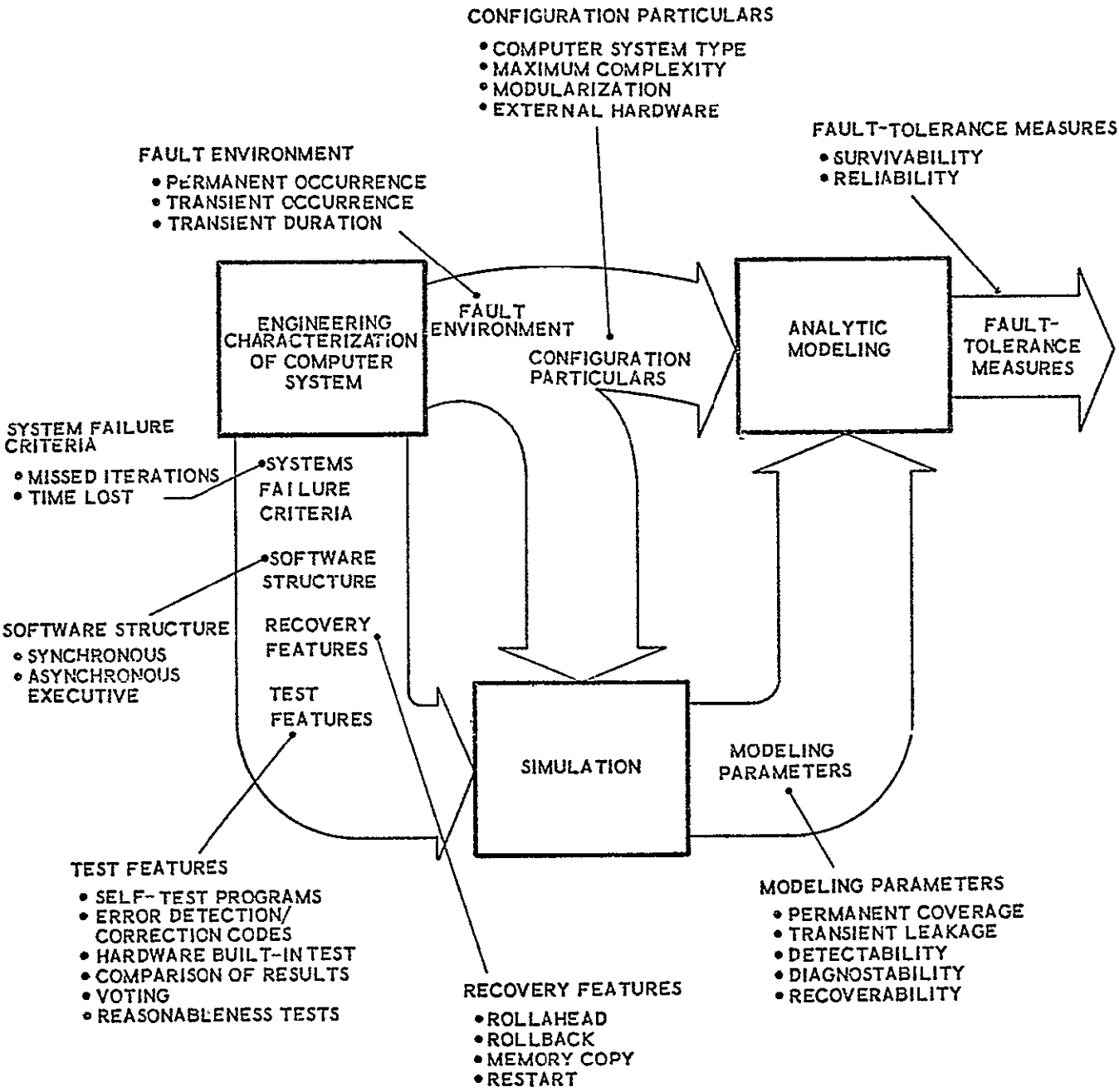


FIGURE 2.2-1 CAST ACTIVITY SEQUENCE AND INFORMATION FLOW

3.0 SHUTTLE (ALT) DATA PROCESSING SUBSYSTEM

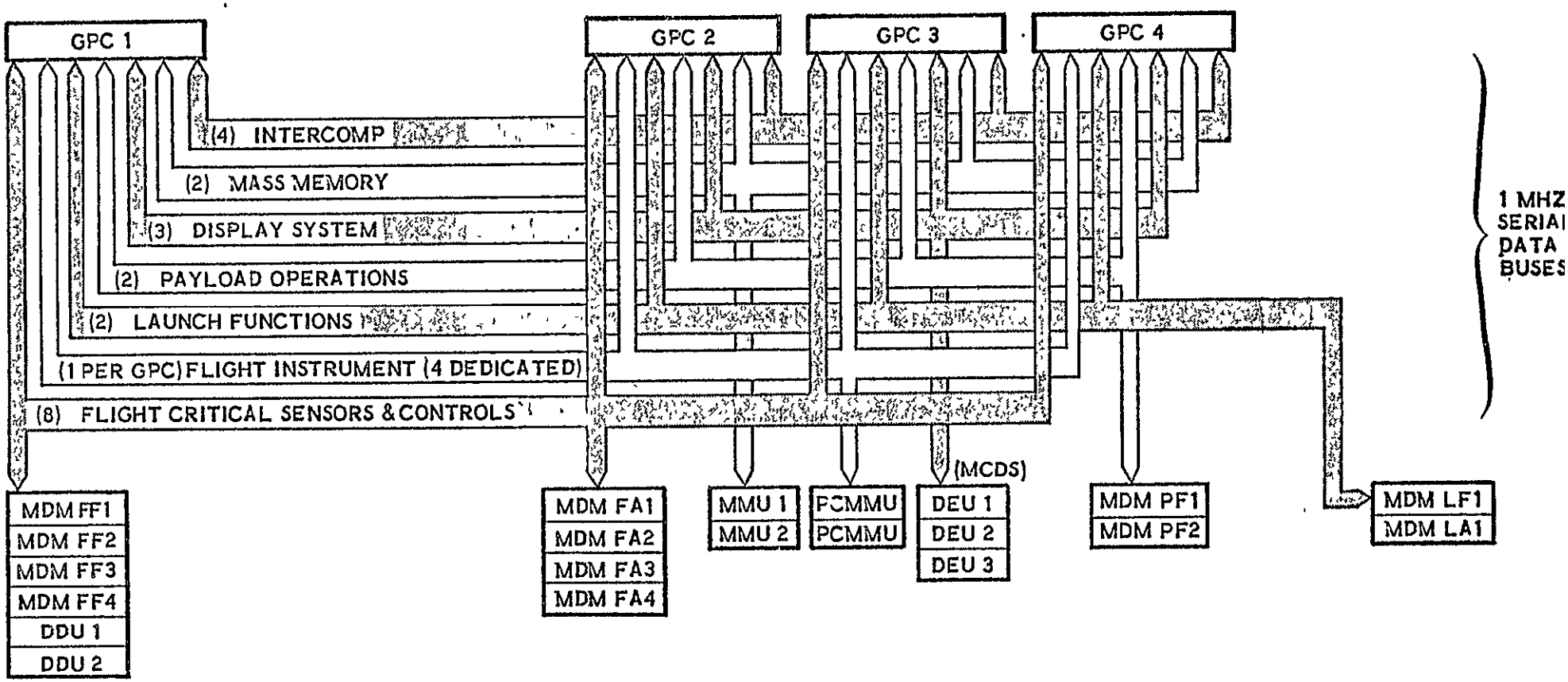
The Shuttle (ALT) Data Processing Subsystem was modeled on the basis of information in various Rockwell and IBM descriptive documents.

The Shuttle (ALT) Data Processing Subsystem is composed of five, identical, general-purpose digital computers. Each of the five are capable of communicating with the peripheral equipment to perform both flight-critical and non-critical functions. During the approach-landing test, four of these computers operate in concert, receiving the same input data, performing the same flight-critical computations, and transmitting the same output commands. Recovery time during ALT is intended to be less than one second. The fifth GPC, i.e., the one supplying signals to the back-up flight control system, is not included since it is only used in ALT if a software error is detected and these errors are not modeled during this phase of the work. The DPS is shown diagrammatically on the facing page.

As shown in the figure, communication among the GPCs, and between the GPCs and/or the peripheral devices is effected through use of seven groups of buses. The number of buses in each group is shown on the figure. Each of these buses is a one megahertz, serial bus. Communications between units on a bus is accomplished through use of command words, command data words, and response data words. Each GPC is composed of a central processing unit (CPU) and an input-output processor (IOP). All information transfers to and from the GPCs are handled through the IOP. Software control is used to instruct each bus within a data-bus group whether it is to operate in the command or listen mode. When operating in the command mode, data requests and commands are sent to the peripheral equipment and the data is then supplied over the same bus. When in the listen mode, data are only received on the bus.

The bus configuration allows each computer to have access to all flight-critical data received or transmitted by the other computers. Each of the redundant subsystems is connected to a different bus. Hence for data input, a different computer requests data from each of the subsystems. The requested data are then available to all other computers. Thus identical input data are available to each computer in the DPS.

For data output, since each channel of the actuator subsystem is connected to a different bus of the group, a different computer transmits command data to each of the voting actuator channels. As a result of the bus-computer



SHUTTLE ORBITER COMPUTER SYSTEM BLOCK DIAGRAM (ALT)

interconnections, each computer can monitor the command data sent out by each of the other computers.

When data is to be transferred between computers, each computer communicates with all other computers through the inter-computer communication (ICC) buses. Only the GPCs are connected to the ICC buses. In order to avoid data skew of either inputs or outputs, synchronization is accomplished in the DPS through use of inter-computer discrete signals and synchronization software.

Sensors and actuators are connected to the appropriate bus through multiplex-demultiplex (MDM) units. Analog display units are connected to their bus through display driver units (DDU), while the multifunction CRT display system (MCDS) is connected through display electronic units (DEU). The mass memory units (MMU) and pulse code modulation master units (PCMMU) are connected directly to their respective buses.

The actual free-flight portion of ALT lasts approximately 172 seconds. However, for mission success probability calculations, the mission time can be thought of as starting 4.5 hours before takeoff of the Shuttle carrier aircraft (SCA) and lasting until 86 minutes after takeoff for a total time of just under six hours.

Fault detection in the Shuttle DPS GPCs is accomplished through use of the five techniques shown in Table 3.0-I. The compare-word-sum check involves summing critical GPC actuator-command outputs, and each GPC comparing its sum with that of the others. This check is performed each computation cycle. This comparison is performed by use of the Fault Detection Identification Program. If the difference is greater than that allowable and has occurred the maximum permissable number of times, then the fail-discrete of the faulty GPC is set.

There are two recovery approaches available in the Shuttle GPC configuration. The first of these is one in which the crew identifies a failed GPC through use of the "failed-discrete" and may either switch out the failed machine or try an initial program load (IPL). The IPL approach is used when there is reason to believe that a transient fault has been experienced. The second recovery approach is to crew-enable inhibition of transmission of outputs from the failed GPC. This inhibition is accomplished automatically once it has been enabled by the crew. It should be noted that restoration of a GPC that may have suffered a transient is not attempted during the action portion of ALT. This is because of the stringent recovery time constraints and the

fact that restoring and adding a computer to the redundant set during time-critical mission phases requires a significant amount of computer memory and time and introduces greater than desirable operational complication.

Fault detection in the peripheral units of the DPS is accomplished by a combination of BITE and GPC-supervised tests. The recovery approach used depends upon the particular unit.

TABLE 3.0-I FAULT DETECTION, LOCATION AND RECOVERY ACTIONS

Function	Action/Indication
Fault Detection	Compare word sum check Bus channel timeout test Built-in-test equipment Self-test programs Watchdog timer
Fault Location	Failure-vote-discrete output GPC-fail-discrete output
Recovery	Try crew-enabled IPL Inhibit output transmission

4.0 ANALYTIC MODEL MODIFICATION

4.1 SHUTTLE AVIONICS SYSTEM PARTITIONING

4.1.1 GENERAL

Partitioning the Shuttle avionics system has a two-fold purpose. First, the system must be subdivided into independent module sets. Second, the module sets should be sufficiently simple for mathematically tractable solutions.

By independence of module sets, we mean independence with respect to the impact of faults from one set to the other. A definition of independence is as follows: Given a collection of module sets, the sets are independent of each other if a faulty module within one set does not incapacitate modules within any other set. However, within each independent module set, a failure of one module type has an effect on other module types. For example, a CPU fault would cause its IOP to not function properly, and an MDM failure would prevent access to the devices it services.

Having defined the independent partitions, the survivability of each partition may be determined independently and the system survivability is the product of the survivabilities of the partitions.

The first-cut partitions are along the lines of the bus groups. These groups are: the four general-purpose computers (GPC); the flight-critical buses and connected equipment (FCB); the two mass memory units and their buses (MM); the display equipment and their buses (MCDS); the payload operations equipment and buses (PLO); the launch-related equipment and buses (LE); and the flight instrumentation and buses (PCM). The back-up system is not considered here. Modeling it involves consideration of the probability of a software fault and its detectability.

A failure of one of these groups has a different impact on the Shuttle mission depending on the group. There are two levels of failure criticality: safety critical and mission critical. Safety critical failures threaten the Shuttle vehicle and the lives of the crew while mission critical failures affect the accomplishment of mission. A bus group falls into one of these two categories. The safety critical partitions for ALT are: the GPCs, the flight-critical bus group, and the MCDS. A safety critical failure is also mission critical since a lost vehicle implies an unsuccessful mission. Therefore,

safety critical partitions are also mission critical. The flight instrumentation is mission critical, while the remaining bus groups are not applicable to ALT.

- GENERAL-PURPOSE COMPUTER GROUP
- FLIGHT-CRITICAL-BUSES AND RELATED EQUIPMENT
- MASS MEMORY EQUIPMENT GROUP
- DISPLAY EQUIPMENT
- PAYLOAD OPERATIONS EQUIPMENT
- LAUNCH-RELATED EQUIPMENT
- FLIGHT INSTRUMENT EQUIPMENT

THE SHUTTLE AVIONICS SYSTEM HAS BEEN PARTITIONED INTO THESE SEVEN INDEPENDENT EQUIPMENT GROUPS

4.1.2 DETAILED PARTITIONING

The approach utilized in arriving at the partitioning described in the previous topic involves first a partitioning along functional unit boundaries, and then a checking for fault interactions. If fault interactions are not found, the partitioning stands. Otherwise a re-partitioning is required. It is desirable to refine the partitions into as many smaller parts as possible to make the analysis of each as simple as possible.

THE GPCs

The GPC is composed of a CPU, memory, and IOP. A failure in any one of these areas interferes with the correctness of program execution or output data. One may say that an individual MIA failure in the IOP affects only the associated bus, and thus the GPC is still capable of performing functions that do not require the services of the affected bus. However, the present recovery prodedures do not take this into account at the present time. Also, an MIA represents a very small portion of the total GPC failure rate. Thus to a reasonable approximation the set of GPC's is a partition.

THE FLIGHT CRITICAL BUSES AND RELATED EQUIPMENT

The flight critical bus system consists of 8 buses connected to 4 forward MDMs, 4 aft MDMs and 2 DDUs. Failures in one of these module groups does not affect the other module groups. Bus failures do affect more than one module group, but the bus failure rate is very small compared to those of the modules. Because it is small, the bus failure rate can be included with each of the module groups with a very small resultant error. The result is a slightly pessimistic estimation of the survivability. Therefore the forward MDMs, aft MDMs, and DDUs, with the buses attached to each, constitute three more partitions.

FLIGHT INSTRUMENTATION

The flight instrumentation consists of the PCM masters, OI buses, and OF and OA MDMs. An OI bus is dedicated to a PCM master while each of the OF and OA MDMs may use either bus. Thus the partitions generated are: PCM master plus OI buses, OF MDMs, and OA MDMs.

OTHER PARTITIONS

There are four additional partitions. These are the mass memories, the displays (MCDS), the payload operations equipment, and the launch-related equipment.

Because each of these have independent buses that are not used by other module groups, they can each be considered as independent partitions. Only the MDCS is used in ALT.

The safety critical and mission critical survivabilities are the product of the individual partition survivabilities.

$$S_S = S_{GPC} \times S_{MCDS} \times S_{FF} \times S_{FA} \times S_{DDU}$$

and $$S_M = S_S \times S_{PCM} \times S_{OF} \times S_{OA}$$

where S_S = Safety critical survivability

S_M = Mission critical survivability

and the remaining subscripts pertain to the mnemonics of the partitions.

SAFETY CRITICAL

1. GPCs and Intercomputer Buses
2. FF MDMs and All Flight Critical Buses
3. FA MDMs and FC Buses 5-8
4. DDUs and FC Buses 1-4
5. MCDs and Display Buses

MISSION CRITICAL

1. PCM Master and OI Buses
2. OF MDMs
3. OA MDMs
4. Safety Critical Group

SHUTTLE PARTITIONS FOR ALT

4.2 GPC MODELING

4.2.1 STATE DIAGRAM DERIVATION

The GPC model is directly applicable to all of the partitions except for the flight critical bus partitions and the MCDS. Specifically, it models the case where a fault anywhere in a string fails the entire string. It is also useful as an approximation when this is not the case.

Prior developments of this model assumed a detection probability of unity because fault detection was in all cases (except residual simplex) accomplished by voting or comparison. The use of fault detectors such as BITE or self test require the addition of imperfect detectability to the analytic model.

The state diagram shown in Figure 4.2-1 demonstrates the sequence of events taking place in a module set undergoing faults. We begin at time T=0 in the N fault-free modules state and find the probability of the module set failing as a function of time. Faults occur at a rate $\lambda+\tau$, the sum of the permanent and transient fault rates. After a fault occurs, we move to the detection state. With probability U_N, the detectability, the fault is detected, and we move to the transient recovery state. Failure to detect the fault is assumed to pollute the system with errors resulting in a system failure. After detection, a transient recovery is attempted. If transient recovery is successful, the module set is restored to N working units. Transient recovery is unsuccessful if the fault is permanent or with probability ℓ_N (transient leakage) if the fault is transient. The unsuccessful transient recovery leads to a permanent recovery procedure where either a spare is added or the module set redundancy is reduced by one. Failure of permanent recovery results in system failure.

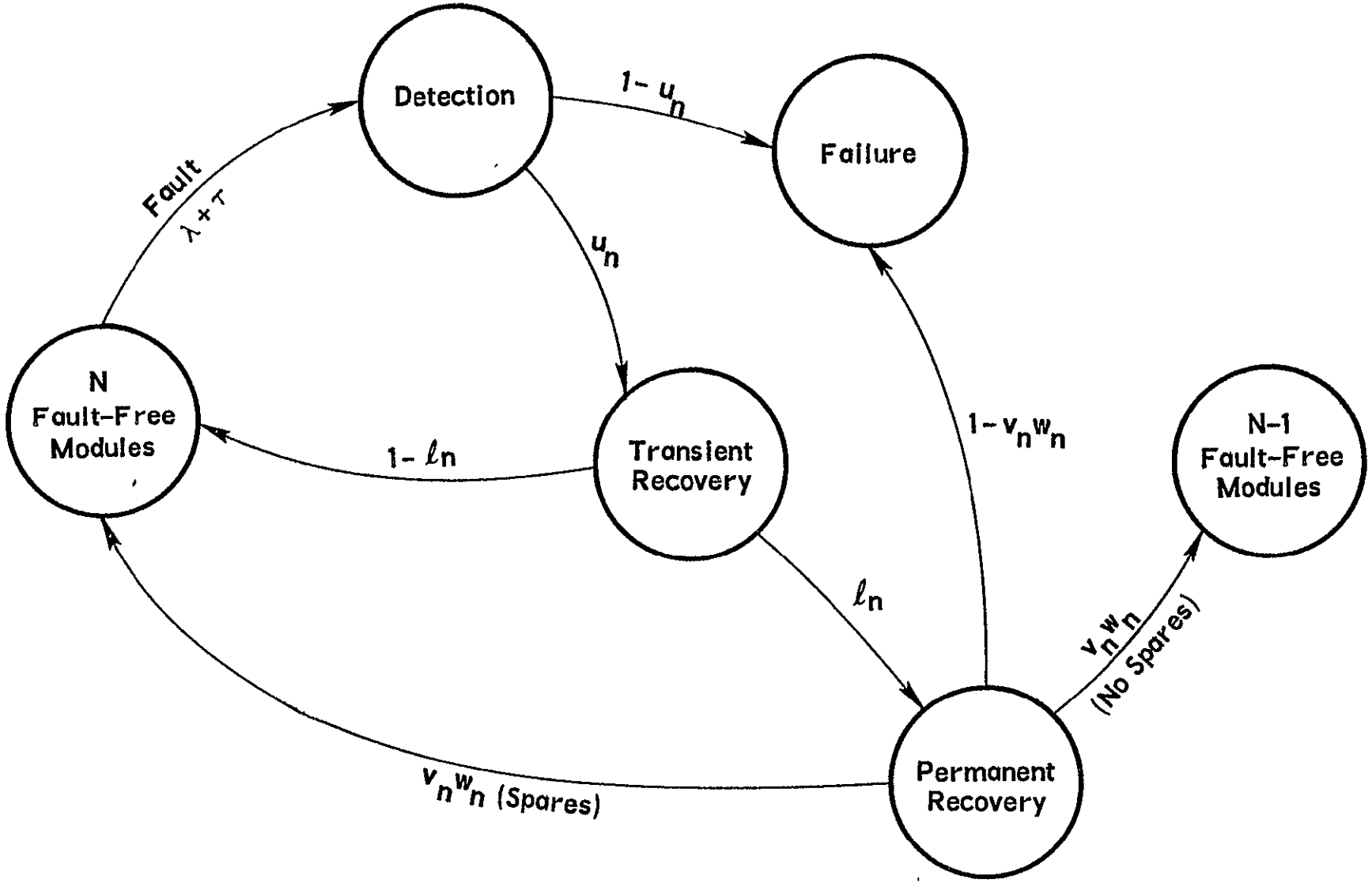


FIGURE 4.2-1 FAULT OCCURRENCE/RECOVERY STATUS STATE DIAGRAM

4.2.2 FORMULATION AND SOLUTION OF EQUATIONS

The probability of system failure is the sum of the probability of failing through three mutually exclusive failure paths. The three ways to fail are:

1. Failure to detect
2. Incorrect isolation or faulty permanent recovery
3. Failure from N - 1 fault-free modules

The probability of failure as a function of mission time then becomes:

$$F_N(T) = (1-u_N) \int_0^T N\sigma_t e^{-N\delta_N t} dt$$

$$+ (1-v_N w_N)\, u_N \int_0^T N\sigma_N e^{-N\delta_N t} dt$$

$$+ u_N v_N w_N \int_0^T N\sigma_N e^{-N\delta_N t} F_{N-1}(T-t)dt$$

where the terms used in the expression are defined on the opposite page. Integrat the first two terms, replacing t with T-t in the third term, letting $C_N = u_N v_N w_N$, and simplifying, we have

$$F_N(T) = \left(1- \frac{C_{N\sigma N}}{\delta_N}\right)\left(1-e^{-N\delta_N T}\right)$$

$$+ NC_N\sigma_N e^{-N\delta_N T} \int_0^T e^{N\delta_N t} F_{N-1}(t)dt$$

Replacing $F_N(T)$ and $F_{N-1}(T)$ with $1-S_N(T)$ and $1-S_{N-1}(T)$, respectively and rearrangi terms, we have

$$S_N(T) = e^{-N\delta_N T} + NC_N\sigma_N e^{-N\delta_N T} \int_0^T e^{N\delta_N t} S_{N-1}(t)dt$$

This integral equation may be solved recursively by assuming $S_N(T)$ is a sum of exponentials

$$S_N(T) = \sum_{k=1}^{N} \sigma_{Nk} e^{-k\delta_K T}$$

Substituting for $S_{N-1}(T)$ in the above integral equation, performing the integration and simplifying yields

$$S_N(T) = \left(1 - \sum_{k=1}^{N-1} \frac{NC_N\sigma_N\alpha_{N-1k}}{N\delta_N - k\delta_k}\right) e^{-N\delta_N T}$$

$$+ \sum_{k=1}^{N-1} \frac{NC_N\sigma_N\alpha_{N-1k}}{N\delta_N - k\delta_k} e^{-k\delta_k T}$$

From this we can identify the recussive definition of the α's as follows:

$$\alpha_{Nk} = \frac{NC_N\sigma_N\alpha_{N-1}k}{N\delta_N - k\delta_k} \qquad k = 1,\ldots, N-1$$

$$\alpha_{NN} = 1 - \sum_{k=1}^{N-1} \alpha_{Nk}$$

These equations show the parameter set required for the analytic model.

TABLE 4.2-I PARAMETER DEFINITIONS

ℓ_N = Transient leakage (probability of failure of transient recovery given fault is transient)

u_N = Detectability (probability fault is detected given fault occurs)

v_N = Diagnosability (probability fault is properly isolated given fault is detected)

w_N = Recoverability (probability system recovers given fault is properly isolated)

C_N = $u_N v_N w_N$ Coverage (probability system recovers given fault occurs)

σ_t = $\lambda + \tau$ Transient plus permanent failure rate

σ_N = $\lambda + \ell_N\tau$ Permanent and leaky transient rate

δ_N = $u_N\sigma_N + (1-u_N)\sigma_t$ Rate of faults resulting in failure or redundancy degradation

4.3 MCDS MODELING

4.3.1 STATE DIAGRAM DERIVATION

The multifunction computer display system (MCDS) is a special case to be modeled. It consists of the display electronics unit (DEU), display unit (DU) and keyboard (KB). The DU is dedicated to the DDU, so we consider it a part of the DEU for analysis purposes. There are two KBs connected to three DEUs by a switching arrangement. The switches allow three configurations as follows:

1. KB A ⟷ DEU A
   KB B ⟷ DEU B
2. KB A ⟷ DEU A
   KB B ⟷ DEU C
3. KB A ⟷ DEU C
   KB B ⟷ DEU B

This connection arrangement is illustrated in Figure 4.3-1. The fault occurrence/recovery status state diagram is given in Figure 4.3-2. At the beginning of the mission, the MCDS is in the no faults state. If a keyboard fails, one of the DEUs will be permanently deprived of a keyboard. The mission continues with a simplex keyboard and duplex DEUs. If DEU C fails, then KB A will be dedicated to DEU A, and KB B will be dedicated to DEU B for the remainder of the mission. If DEU A or B fails first, then one KB is dedicated to DEU C while the other may be connected to either DEU C or B (we assume A was the failed DEU). There are four possibilities for the next failure: (1) If the dedicated KB fails then the common KB may serve the remaining DEUs. We have a simplex keyboard and a duplex DEU. (2) If the common keyboard fails, then DEU B has no access to a KB. We complete the mission in simplex. (3) If DEU C fails, the dedicated KB has no DEU to serve or (4) If DEU B fails; then we complete the mission with duplex KBs and simplex DEU.

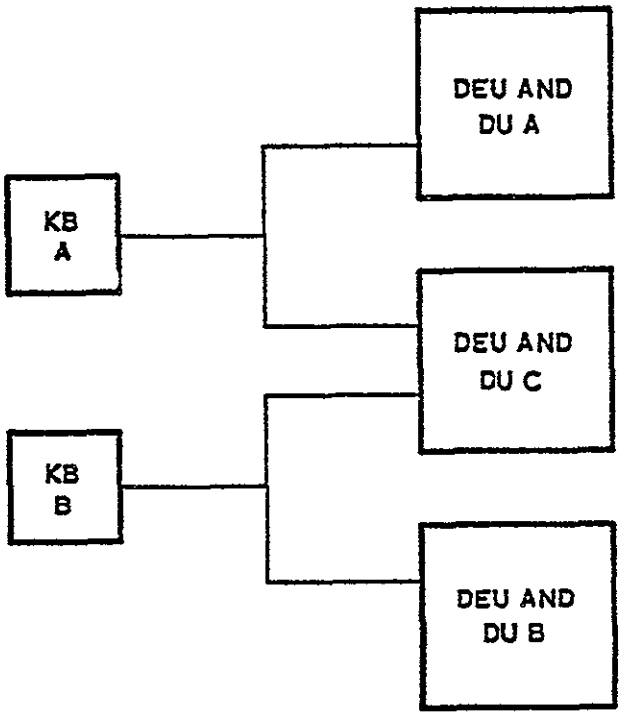


FIGURE 4.3-1 SYMBOLIC INTERCONNECTION DIAGRAM OF THE MCDS

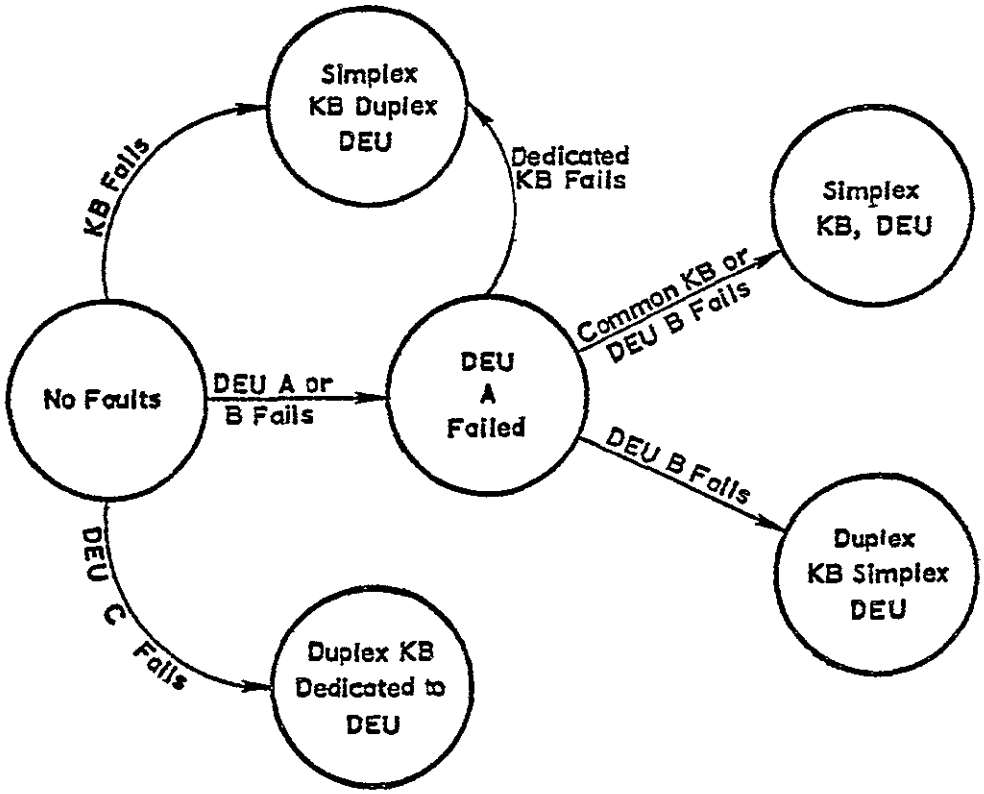


FIGURE 4.3-2 FAULT OCCURRENCE/RECOVERY STATUS STATE DIAGRAM FOR THE MCDS

4.3.2 EQUATION DERIVATION

The quantities used in the derivation that follows are given on the opposite page. The survivability is the sum of four mutually exlcusive probabilities as can be seen from the state diagram of Figure 4.3-2.

1. No failures occur.
2. The first failure is to DEU A or B, the system survives any subsequent faults.
3. The first failure is to a KB, the system survives any subsequent failures.
4. The first failure is to DEU C, the system survives subsequent faults.

By using the general expressions for simplex and duplex survivability, S(T) then becomes

$$S(T) = S_{23}(T) + 2\,C_{d3}\sigma_{d3}S_{23}(T)\int_0^T S_{DEU\ FAILED}(t)/S_{23}(t)\,dt$$

$$+ 2\,C_{k2}\sigma_{k2}S_{23}(T)\int_0^T\left[\frac{2\,C_{d2}\sigma_{d2}}{2\delta_{d2}-\delta_{d1}}S_{11}(t) + \left(1 - \frac{2\,C_{d2}\sigma_{d2}}{2\delta_{d2}-\delta_{d1}}\right)S_{12}(t)\right]/S_{23}(t)\,dt$$

$$+ C_{d3}\sigma_{d3}S_{23}(T)\int_0^T\left[\frac{2(C_{k2}\sigma_{k2}+C_{d2}\sigma_{d2})}{2(\delta_{k2}+\delta_{d2}) - \delta_{d1}\delta_{k1}}S_{11}(T) + \left(1 - \frac{2(C_{k2}\sigma_{k2}+C_{d2}\sigma_{d2})}{2(\delta_{k2}+\delta_{d2}) - \delta_{k1}-\delta_{d1}}\right)S_{22}(t)\right]/S_{23}(t)$$

The problem is to find $S_{DEU\ FAILED}$. It is the sum of four mutually exclusive probabilities:

1. No more failures.
2. The next failure is to the common KB or to DEU C, and the system survives.
3. The next failure is to the dedicated KB, and the system survives.
4. The next failure is to DEU B, and the system survives.

TABLE 4.3-I SYMBOL DEFINITIONS

* λ = Permanent Fault Rate

* τ = Transient Fault Rate

** u = Detectability

** v = Diagnosability

** w = Recoverability

** C = Coverage, i.e., uvw

** ℓ = Transient Leakage

$\sigma_t = \lambda + \tau$ Total Fault Rate

** $\sigma = \lambda + \ell\tau$ Effective Permanent Fault Rate

** $\delta = u\sigma + (1+u)\sigma_t$

$S_{mn}(t) = \exp[-(m\ \delta_{km} + n\ \delta_{dn})t]$

---

* Quantities marked with an asterisk have a subscript k or d to indicate association with a keyboard or DEU + DU, respectively.

**Quantities marked with a double asterisk have a double subscript kn or dn to indicate n keyboards remaining or n DEU + DUs remaining, respectively.

So $S_{DEU\ FAILED}$ becomes

$$S_{DEU\ FAILED}(T) = S_{22}(T) + (C_{k2}\sigma_{k2}+C_{d2}\sigma_{d2})\ S_{22}(T)\int_0^T S_{11}(t)/S_{22}(t)\ dt$$

$$+ C_{k2}\sigma_{k2}S_{22}(T)\int_0^T \left[\frac{2C_{d2}\sigma_{d2}}{2\delta_{d2}-\delta_{d1}} S_{11}(t) + \left(1 - \frac{2C_{d2}\sigma_{d2}}{2\delta_{d2}-\delta_{d1}}\right) S_{12}(t)\right]/S_{22}(t)\ dt$$

$$+ C_{d2}\sigma_{d2}S_{22}(T)\int_0^T \left[\frac{2C_{k2}\sigma_{k2}}{2\delta_{k2}-\delta_{k1}} S_{11}(t) + \left(1 - \frac{2C_{k2}\sigma_{k2}}{2\delta_{k2}-\delta_{k1}}\right) S_{21}(t)\right] /S_{22}(t)\ dt$$

$$= S_{22}(T) + \frac{C_{k2}\sigma_{k2}+C_{d2}\sigma_{d2}}{2\ \delta_{d2}+2\ \delta_{k2}-\delta_{k1}-\delta_{d1}} \left[S_{11}(T)-S_{22}(T)\right]$$

$$+ \frac{2\ C_{k2}\sigma_{k2}\ C_{d2}\sigma_{d2}}{(2\ \delta_{d2}-\delta_{d1})(2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1})} \left[S_{11}(T) - S_{22}(T)\right]$$

$$+ \frac{C_{k2}\sigma_{k2}}{2\ \delta_{k2}-\delta_{k1}} \left(1 - \frac{2\ C_{d2}\sigma_{d2}}{2\ \delta_{d2}-\delta_{d1}}\right) \left[S_{12}(T) - S_{22}(T)\right]$$

$$+ \frac{2\ C_{d2}\sigma_{d2}\ C_{k2}\sigma_{k2}}{(2\ \delta_{k2}-\delta_{k1})(2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1})} \left[S_{11}(T) - S_{22}(T)\right]$$

$$+ \frac{C_{d2}\sigma_{d2}}{2\ \delta_{d2}-\delta_{d1}} \left(1 - \frac{2\ C_{k2}\sigma_{k2}}{2\ \delta_{k2}-\delta_{k1}}\right) \left[S_{21}(T) - S_{22}(T)\right]$$

Substituting $S_{DEU\ FAILED}$ into the expression for S(T), we have the following result

$$S(T) = S_{23}(T)$$

$$+ \frac{4\ C_{k2}\sigma_{k2}C_{d2}\sigma_{d2}}{(2\ \delta_{d2}-\delta_{d1})(2\ \delta_{k2}+3\ \delta_{d3}-\delta_{k1}-\delta_{d1})}\left[S_{11}(T) - S_{23}(T)\right]$$

$$+ \frac{2\ C_{k2}\sigma_{k2}}{2\ \delta_{k2}+3\ \delta_{d3}-\delta_{k1}-2\ \delta_{d2}}\left(1 - \frac{2\ C_{d2}\sigma_{d2}}{2\ \delta_{d2}-\delta_{d1}}\right)\left[S_{12}(T) - S_{23}(T)\right]$$

$$+ \frac{4\ C_{d3}\sigma_{d3}\ C_{kd}(\sigma_{k2}+\sigma_{d2})}{(2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1})(3\ \delta_{d3}+2\ \delta_{k2}-\delta_{d1}-\delta_{k1})}\left[S_{11}(T) - S_{23}(T)\right]$$

$$+ \frac{C_{d3}\sigma_{d3}}{3\ \delta_{d3}-2\ \delta_{d2}}\left(3 - \frac{4\ C_{kd}(\sigma_{k2}+\sigma_{d2})}{2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1}}\right)\left[S_{22}(T) - S_{23}(T)\right]$$

$$+ \frac{4\ C_{d3}\sigma_{d3}\ C_{k2}\sigma_{k2}\ C_{d2}\sigma_{d2}}{(2\ \delta_{d2}-\delta_{d1})(2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1})}\left[\frac{S_{11}(T) - S_{23}(T)}{3\ \delta_{d3}+2\ \delta_{k2}-\delta_{k1}-\delta_{d1}} - \frac{S_{22}(T) - S_{23}(T)}{3\ \delta_{d3}-2\ \delta_{d2}}\right]$$

$$+ \frac{2\ C_{d3}\sigma_{d3}\ C_{k2}\sigma_{k2}}{2\ \delta_{k2}-\delta_{k1}}\left(1 - \frac{2\ C_{d2}\sigma_{d2}}{2\ \delta_{d2}-\delta_{d1}}\right)\left[\frac{S_{12}(T) - S_{23}(T)}{3\ \delta_{d3}+2\ \delta_{k2}-\delta_{k1}-2\ \delta_{d2}} - \frac{S_{22}(T) - S_{23}(T)}{3\ \delta_{d3}-2\ \delta_{d2}}\right]$$

$$+ \frac{4\ C_{d3}\sigma_{d3}\ C_{d2}\sigma_{d2}\ C_{k2}\sigma_{k2}}{(2\ \delta_{k2}-\delta_{k1})(2\ \delta_{k2}+2\ \delta_{d2}-\delta_{k1}-\delta_{d1})}\left[\frac{S_{11}(T) - S_{23}(T))}{3\ \delta_{d3}+2\ \delta_{k2}-\delta_{d1}-\delta_{k1}} - \frac{S_{22}(T) - S_{23}(T)}{3\ \delta_{d3}-2\ \delta_{d2}}\right]$$

$$+ \frac{2\ C_{d3}\sigma_{d3}\ C_{d2}\sigma_{d2}}{2\ \delta_{d2}-\delta_{d1}}\left(1 - \frac{2\ C_{k2}\sigma_{k2}}{2\ \delta_{k2}-\delta_{k1}}\right)\left[\frac{S_{21}(T) - S_{23}(T)}{3\ \delta_{d3} - \delta_{d1}} - \frac{S_{22}(T) - S_{23}(T)}{3\ \delta_{d3}-2\ \delta_{d2}}\right]$$

4.4 FLIGHT CRITICAL BUS MODELS

4.4.1 GENERAL

The flight critical bus partitions present a difficult modeling problem due to the fact that an MDM or DDU failure fails the entire string, while a device failure does not necessarily mean a string failure. For example, if MDM FF1 fails to function, the GPCs are no longer able to access the devices dedicated to FF1. On the other hand, if accelerometer 1 fails, MDM FF1 may still communicate with the remaining devices in the string. Thus the device types are dependent in pairs, but are in actuality dependent through the MDMs or DDUs.

The modeling technique used in the previous sections results in mathematically intractable formulations when applied to this situation. However an approximate model becomes appropriate to cross check with the flight critical bus simulation, and to provide rapid and economical results after a successful cross check. There are two approximations possible with the previous modeling technique. One approach involves assuming complete unit independence and the other is to assume total unit dependence. These represent an upper and a lower bound, respectively to the true survivability. An intermediate solution that provides realistic, usable results may be obtained by taking each of the mutually exclusive cases of MDM or DDU failure combinations and modeling the remaining device's survivability, given that failure combination. Each possible combination that can result in a successful mission is modeled. As an example of one of these combinations, suppose MDM FF1 fails and the other FF MDMs survive, then the ADTA must survive the mission in triplex while the other device types must survive in duplex.

By fixing the failure conditions of the interfaces (MDMs and DDUs) that make the devices dependent, we have removed the cause of the dependence of the devices. A further exposition of this method is contained in the sections that follow.

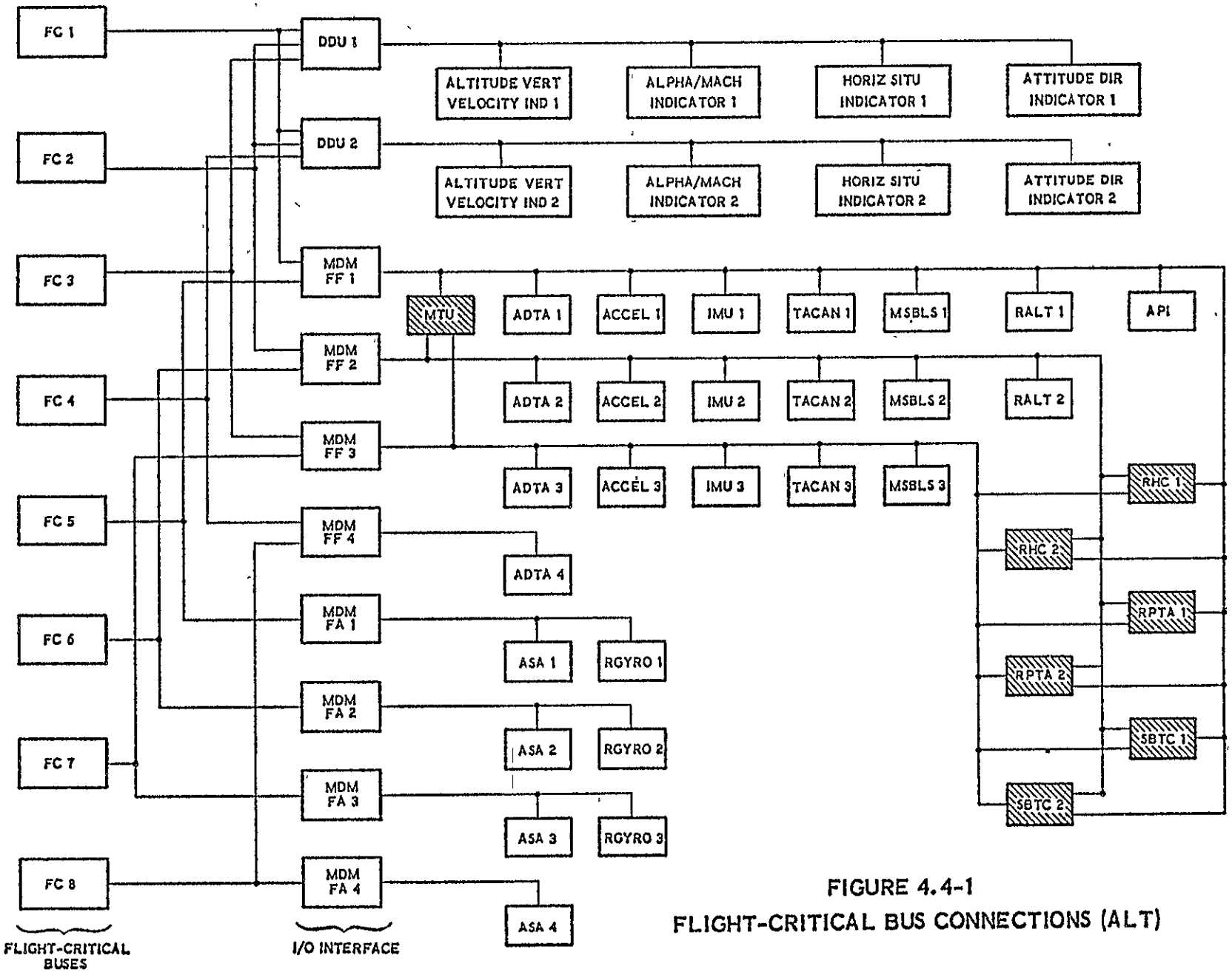


FIGURE 4.4-1
FLIGHT-CRITICAL BUS CONNECTIONS (ALT)

4.4.2 DDU MODEL DERIVATION

The flight display partition consists of the display drive units (DDUs) driving the altitude vertical velocity indicator (AVI), alpha/mach indicator (AMI), horizontal situation indicator (HSI), and the attitude direction indicator (ADI). There are duplicate display strings. In the modeling of this partition there are two, mutually-exclusive failure conditions of the DDUs that can result in the survival of the displays: none fail or only one fails. If no DDUs fail during the mission then each indicator must survive independently in duplex. And if one DDU fails, each display associated with the non-failed DDU must survive. The display partition survivability becomes the sum of these two survival conditions as follows:

$$S_{DDU} = R_{DDU}^2 \times S_{AVI}^{(2)} \times S_{AMI}^{(2)} \times S_{HSI}^{(2)} \times S_{ADI}^{(2)}$$
$$+ 2C_2 \, R_{DDU}(1-R_{DDU}) \times S_{AVI}^{(1)} \times S_{AMI}^{(1)} \times S_{HSI}^{(1)} \times S_{ADI}^{(1)}$$

where the superscript on S represents the redundancy level that the display must survive from.

The quantity, C_2, is the coverage associated with one DDU failing sometime during the mission. This coverage is not simply the DDU coverage because one or more of the displays on the string may have failed before the DDU. Of course, display failures after the DDU fails have no impact. We need to find

$$P_A = \Pr[\text{device A fails before the DDU, given the DDU fails before T}].$$

The quantity C_2 then becomes

$$C_2 = C_{DDU} \, (1-P_{AVI} + C_{AVI} \, P_{AVI})(1-P_{AMI} + C_{AMI} \, P_{AMI})$$
$$(1-P_{HSI} + C_{HSI} \, P_{HSI})(1-P_{ADI} + C_{ADI} \, P_{ADI})$$

where the subscripts on P correspond to the mnemonics of the displays.

Now P_A is the joint probability of A failing before the DDU and the DDU failing before T, all divided by the probability of the DDU failing before T. So

$$P_A = \Pr[\text{A fails before DDU and the DDU fails before T}]/(1-e^{-\lambda_{DDU}T})$$
$$= \hat{P}_A/(1-e^{-\sigma_{DDU}T})$$

The quantity $\hat{P}_A$ is the integral over the mission time of the product of probability of A failing by t and the probability of the DDU failing between t and t+dt.

$$\hat{P}_A = \int_0^T (1-e^{-\sigma_A t})\, \sigma_{DDU}\, e^{-\sigma_{DDU} t}\, dt$$

$$\hat{P}_A = \frac{\sigma_A\,(1-e^{-\sigma_{DDU} T}) - \sigma_{DDU}\, e^{-\sigma_{DDU} T}\,(1-e^{-\sigma_A T})}{\sigma_A + \sigma_{DDU}}$$

Substituting $\hat{P}_A$ into the expression for P_A and then letting A be the AVI, AMI, HSI, and ADI in the expression for C_2 yields the desired expression for S_{DDU}.

λ = Permanent failure rate

τ = Transient failure rate

$\sigma_{DDU} = \lambda_{DDU} + \ell_{DDU}\, \tau_{DDU}$

$R_{DDU} = e^{-\sigma_{DDU} T}$

$C_2 = u_2 v_2 w_2$

$S_A^{(k)}$ = Unit A survivability with initial redundancy level k

A = Either AVI, AMI, HSI, or ADI

DEFINITION OF SYMBOLS

4.4.3 FLIGHT-CRITICAL-MDM SURVIVABILITY-MODEL DERIVATIONS

The forward and aft flight critical MDMs present a more complicated situation to model. Here the first three MDMs (denoted type 1) serve several identical flight critical devices, while the fourth serves only one device (see Figure 4.4-1). In this case, we consider the survival conditions with six, mutually-exclusive MDM failure configurations as follows:

1. No MDM failures
2. No MDM type-1 failures, MDM 4 fails
3. One MDM type-1 failure, no MDM 4 failure
4. One MDM type-1 failure, MDM 4 fails
5. Two MDM type-1 failures, no MDM 4 failure
6. Two MDM type-1 failures, MDM 4 fails

In each of the cases, the set of devices served by the non-failed MDMs must independently survive the remainder of the mission. Also, the coverage associated with each MDM failure must take into account device failures on the string prior to the MDM failure. In the flight forward case, MDMs 1-4 serve the ADTA while only MDMs 1-3 serve the remaining devices. The resulting flight-forward-survivability expression is as follows:

$$
\begin{aligned}
S_{FF} = {} & R_{M1}^3 \, R_{M4} \, S_{ADT}^{(4)} \, S_{IMU}^{(3)} \, S_{TAC}^{(3)} \, S_{MCS}^{(3)} \, S_{RHC}^{(3)} \, S_{RPT}^{(3)} \, S_{SBC}^{(3)} \\
& + C_4 \, R_{M1}^3 \, (1-R_{M4}) \, S_{ADT}^{(3)} \, S_{IMO}^{(3)} \, S_{TAC}^{(3)} \, S_{MLS}^{(3)} \, S_{RHC}^{(3)} \, S_{RPT}^{(3)} \, S_{SBC}^{(3)} \\
& + 3C_3 \, R_{M1}^3 \, R_{M4} \, (1-R_{M1}) \, S_{ADT}^{(3)} \, S_{IMU}^{(2)} \, S_{TAC}^{(2)} \, S_{MLS}^{(2)} \, S_{RHC}^{(2)} \, S_{RPT}^{(2)} \, S_{SBC}^{(2)} \\
& + 3C_3 \, C_4 \, R_{M1}^2 \, (1-R_{M4})(1-R_{M1}) \, S_{ADT}^{(2)} \, S_{IMU}^{(2)} \, S_{TAC}^{(2)} \, S_{MLS}^{(2)} \, S_{RHC}^{(2)} \, S_{RPT}^{(2)} \, S_{SBC}^{(2)} \\
& + 3C_3 \, C_2 \, R_{M1} \, R_{M4} \, (1-R_{M1})^2 \, S_{ADT}^{(2)} \, S_{IMU}^{(1)} \, S_{TAC}^{(1)} \, S_{MLS}^{(1)} \, S_{RHC}^{(1)} \, S_{RPT}^{(1)} \, S_{SBC}^{(1)} \\
& + 3C_4 \, C_3 \, C_2 \, R_{M1} \, (1-R_{M4})(1-R_{M1})^2 \, S_{ADT}^{(1)} \, S_{IMU}^{(1)} \, S_{TAC}^{(1)} \, S_{MLS}^{(1)} \, S_{RHC}^{(1)} \, S_{RPT}^{(1)} \, S_{SBC}^{(1)}
\end{aligned}
$$

where each term corresponds to an MDM failure condition given above. In the flight aft case, MDMs 1-4 serve the ASA while only MDMs 1-3 serve the rate gyros. Similarly, the aft survivability becomes:

$$
\begin{aligned}
S_{FA} = {} & R_{M1}^{3}\, R_{M4}\, S_{ASA}^{(4)}\, S_{GNR}^{(3)} \\
& + C_4\, R_{M1}^{3}\, (1-R_{M4})\, S_{ASA}^{(3)}\, S_{GYR}^{(3)} \\
& + 3\, C_3\, R_{M1}^{2}\, R_{M4}\, (1-R_{M1})\, S_{ASA}^{(3)}\, S_{GYR}^{(2)} \\
& + 3\, C_3\, C_4\, R_{M1}^{2}\, (1-R_{M4})(1-R_{M1})\, S_{ASA}^{(2)}\, S_{GYR}^{(2)} \\
& + 3\, C_3\, C_2\, R_{M1}\, R_{M4}\, (1-R_{M1})^2\, S_{ASA}^{(2)}\, S_{GYR}^{(1)} \\
& + 3\, C_4\, C_3\, C_2\, R_{M1}\, (1-R_{M4})(1-R_{M1})^2\, S_{ASA}^{(1)}\, S_{GYR}^{(1)}
\end{aligned}
$$

$R_{M1} = e^{-\sigma_{M1} T}$; M1 denotes MDMs 1 through 3

$R_{M4} = e^{-\sigma_{M4} T}$; M4 refers to MDM 4

$S_A^{(k)}$ is the survivability of the device with mnemonic A with initial redundancy level k.

C_k is the coverage associated with an MDM failure, taking into account devices failing defore the MDM at redundancy level k.

C_4 is the coverage associated with MDM 4 failing.

DEFINITION OF SYMBOLS

5.0 SIMULATOR

5.1 SIMULATOR BACKGROUND AND MODIFICATIONS

5.1.1 BACKGROUND - RCS SIMULATOR

The RCS simulator was developed to provide parameters, which could not be estimated directly, to the analytic model.

The use of simulation studies to investigate the behavior of computer hardware/software systems is well-established. Simulation is used for those situations which are intractable to an analytic approach, or for which the essence is lost when the prerequisite abstractions and simplifying assumptions necessary to the analytic technique are made.

Much attention has been given to improving the mission success probability (MSP) of computer systems by the addition of protective redundancy. Such redundancy allows the system to continue correct operation in the presence of one or more failed components. The efficacy of this improvement is measured by the MSP increase.

The mission success probability is defined as the probability that, given that there were no failed components or erroneous memory information present at mission inception, the hardware and software are operating correctly at the end of the mission. Thus the system must be able to survive both permanent and transient faults.

In order to make an accurate analytic determination of the MSP of this type of system, all fault-tolerance processes (e.g., detection, recoveries, etc.) must be modeled. However, for even a reasonable approximation to a real-world implementation, a mathematical model soon becomes intractable. Simulation is then the alternative solution.

The goal in the RCS work was an approach that is applicable to a wide variety of computer designs, and one which reflects the hardware-software interaction. Thus, a logic-level simulation would provide needless detail, in addition to sacrificing versatility. Hence, a modeling level of detail was chosen that permits description of system details, but is versatile enough to accommodate different computers and configurations.

Translating these ideas into RCS simulation objectives yielded the following three items. The simulator should produce: (1) the fault-tolerance of each of a wide variety of reconfigurable computer system configurations;

(2) global parameters for use in analytic modeling; the (3) the behavior of a configuration in various fault environments.

The requirements imposed on the simulator design by these three objectives are examined in the following paragraphs.

The simulator should be able to produce the desired measures of fault-tolerance for a wide variety of configurations. This requirement can be satisfied in a reasonable way by structuring the simulator such that the various fault-detection and recovery algorithms are implemented as subroutines. Thus a configuration can be described by specifying the applicable set of subroutines, plus the necessary parameters. This simulator structure provides versatility and modularity, and minimizes the impact of addition of new subroutines.

Global parameters are those required when using the analytic model for analysis of a configuration. For example, the transient coverage in triplex, C_T, has been defined as the conditional probability that a triplex system recovers, given that a transient has occurred. If a configuration is analyzed by mathematical modeling, C_T is one of the input parameters of the model. However, it is difficult for the designer to evaluate C_T, since it may depend on: the location of the transient fault; their occurrence rate τ; the time between occurrence and detection of a fault; and the recovery algorithm used. By introducing these factors into the simulation and gathering statistics describing the computer system reaction to transient faults, C_T can be estimated by computing the ratio of the number of successful recoveries from transient faults to the total number of transients.

Thus, for the configurations where the mathematical modeling is applicable, one simulation run gives an estimate of these parameters of the modeling. Then using the model, the MSP of the configuration can be easily determined for any given time t.

The fault environment provided in the simulator should be sufficiently versatile to provide all expected possibilities to test the recovery algorithm utilized in the configuration under simulation. Thus low or high failure rates, existence and duration of transient bursts, long transients, mathematical fault-distribution functions, etc., must be provided. Implementation of this fault environment should be accomplished so as to provide maximum flexibility of environment choice by the user.

5.1.2 EXTENSION OF RCS WORK

The simulator for the Shuttle Data Processing Subsystem is based on the RCS simulator. The basic simulator structure is the same, but nearly all of the programs have been modified and 32 programs have been added. The major effort was spent on the flight-critical bus partition simulation, as this had to be developed from scratch. The shuttle DPS software utilizes a transient recovery procedure that was not postulated in the RCS simulator. A methodology for the simulation of this recovery procedure had to be developed. The flexibility of the simulator was increased by making all transient recovery procedures optional. Other changes include improvements to the simulator I/O format and the replacement of most source statements that are incompatible with the UNIVAC 1108 Fortran compiler.

The flight-critical bus subsystem was partitioned into six classes for separate simulation of faults occurring in: the flight-critical buses, the bus terminal units (MDMs and DBUs), devices directly interfaced with the DDU, dedicated devices directly interfaced with the FF-MDMs, non-dedicated devices interfaced with the FF-MDMs, and devices interfaced with the FA MDMs. A main routine determines in which equipment group the fault occurs and transfers control to the appropriate simulation routine. These routines utilize FCB redundancy and interconnection arrays to determine the impact of the fault on the system. The arrays are then updated to reflect the new system status.

The RCS STATE simulation subroutines were modified in order that the FCB simulation could be included with GPC simulation. Here a routine FIFAU, which is always invoked upon a fault occurrence, was modified to invoke the FCB simulation routines for faults located in the FCB partition. It was necessary to modify the interface to FIFAU in all of the state simulation subroutines.

FCOS uses a different recovery procedure than was postulated in the RCS work. Upon the occurrence of a fault, it is recorded, but no recovery action is taken. If the fault recurs within a certain time window, it is assumed to be permanent, and the system is reconfigured. With this procedure, transient faults whose ill effects disappear after a small time interval do not cause unnecessary system degradation. This recovery procedure had to be modeled and implemented in the simulator program. It was implemented by modifying STATE 2 and STATE 8 of the simulator programs. In addition, the simulator was given more versatility by making all recovery techniques optional.

The simulator input deck had to be modified because several new parameters were introduced. In the process it was set up to use a more uniform structure in order that the chance of error could be decreased. The output format has been modified to include only the pertinent parameters in the configuration summary and to include confidence intervals for simulator statistics.

5.2 GENERAL DISCUSSION OF THE SIMULATOR

5.2.1 SIMULATOR CHARACTERISTICS

A fault-driven simulation that permits multiple simulation runs with one submission has been designed.

Certain aspects of the general approach to the design of the simulator are implicit in objectives 1 and 3 listed in Section 5.1.1, namely the need for versatility and flexibility. There is a third, as-yet-unstated requirement, and that is for an efficient implementation that results in a reasonable computer-cost per run.

The versatility and flexibility requirements can be satisfied by designing a modular simulator that is easily modified (flexibility), and that models many configuration and fault-environment possibilities (versatility). Since we are concerned with behavior of the computer system following occurrence of a fault, we can obtain an efficient implementation by designing a "fault-driven" simulator, rather than one that simulates the continuous operation of the system. Thus, a fault-driven simulation is one that moves from fault occurrence to fault occurrence, simulating the response of the system to each fault, but not simulating the operation of the system in between.

The modularity of the simulator has been demonstrated as it was converted from the RCS simulator to the GPC simulator. Its versatility is indicated by the fact that it can model eight GPC configuration types, and eight fault-environment possibilities.

The simulator program consists of a collection of FORTRAN IV computer programs (tobe run in a CDC 6600 CYBERNET computer environment) organized and designed to satisfy the simulation objectives. The gross organization of the simulation is presented in Figure 5.2-1. The main routine in charge of directing the processing flow of the simulation is designated the Driver. A collection of subroutines are accessible to the Driver via FORTRAN CALL statements. Each of the computer system states are represented by a subroutine. Other supportive subroutines perform statistics gathering and probability generating functions.

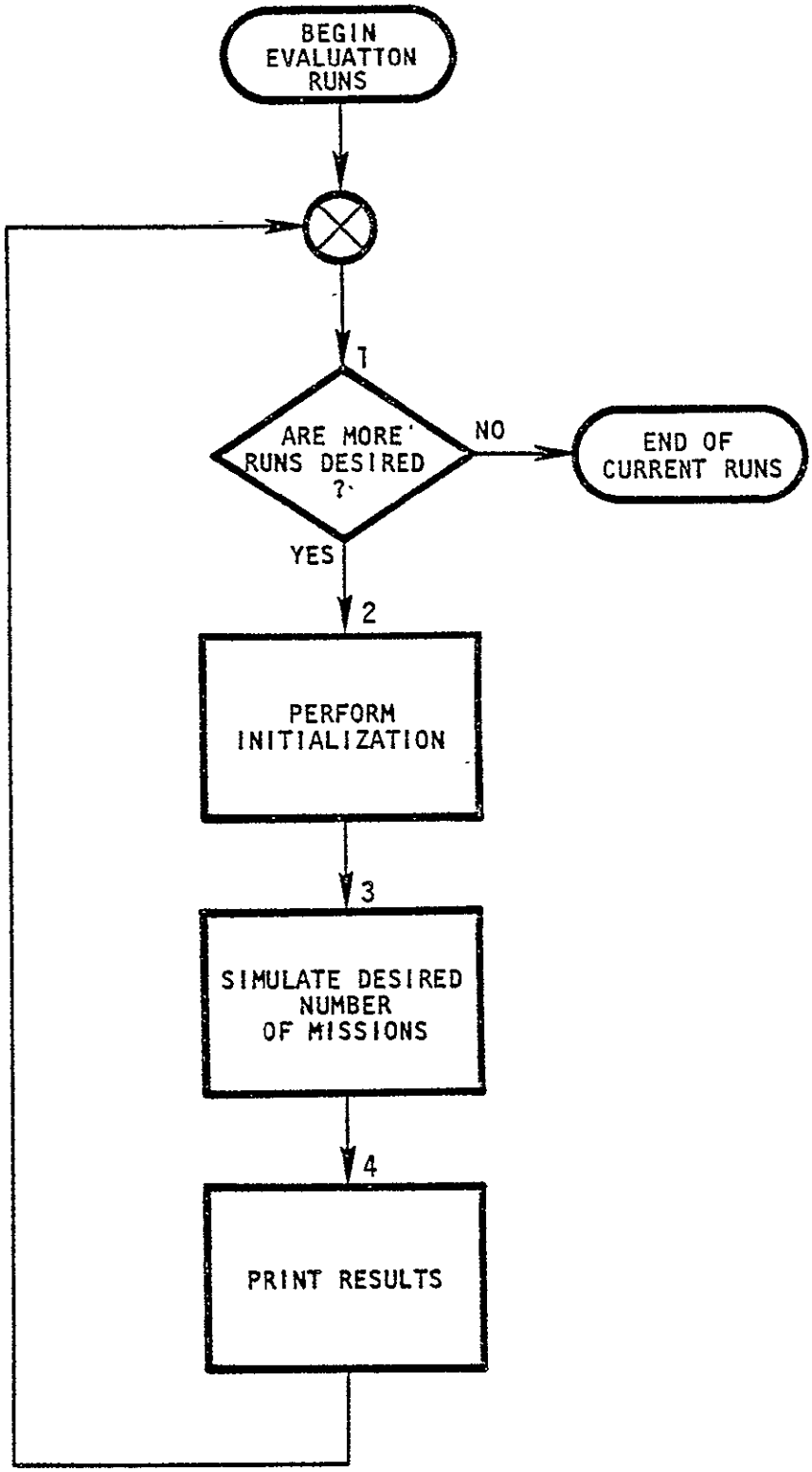


FIGURE 5.2-1 THE RCS SIMULATOR IS STRUCTURED TO PERMIT MULTIPLE RUNS

5.2.2 GLOBAL SIMULATOR ORGANIZATION

The simulator program is structured to simulate the detection of faults within a computer system and the computer system's successful/unsuccessful recovery actions taken in response to the detected faults. Each simulated mission is assigned a mission time. A simulation run consists of the repetitive continued simulation of a designated number of missions (each with the same mission length).

A simulation run consists of several phases. First the system is initialized by obtaining the input parameters and initializing fault counters. Next the system simulation begins. Faults are randomly generated for several missions and placed in a table. The fault table is searched to determine the next mission in which a fault occurs. After the mission parameters are initialized, the handling of faults is simulated. Then the statistics for the mission (i.e. final state, number of faults, causes of failures, etc.) are gathered. This process is repeated until all missions are simulated, and then estimates for analytic model parameters are calculated and printed along with the simulator statistics. Figure 5.2-2 illustrates the process for simulating the required number of missions.

Simulated faults occur in either the GPC partition or the FCB partition. If the fault occurs in the GPC partition it is simulated by one of a set of subroutines dependent upon the current GPC redundancy level and the recovery procedure in progress. This set of subroutines will be identified as the GPC simulation programs in following topics. They are described in more detail in Section 5.3. Faults occurring in the FCB partition are simulated by a subroutine dependent upon the FCB component in which the fault occurs. The status of the FCB subsystem is represented by a set of tables. An approach like that chosen for the GPC simulation was impossible because of the large number of possibilities involved. Section 5.4 describes the FCB simulator programs in detail.

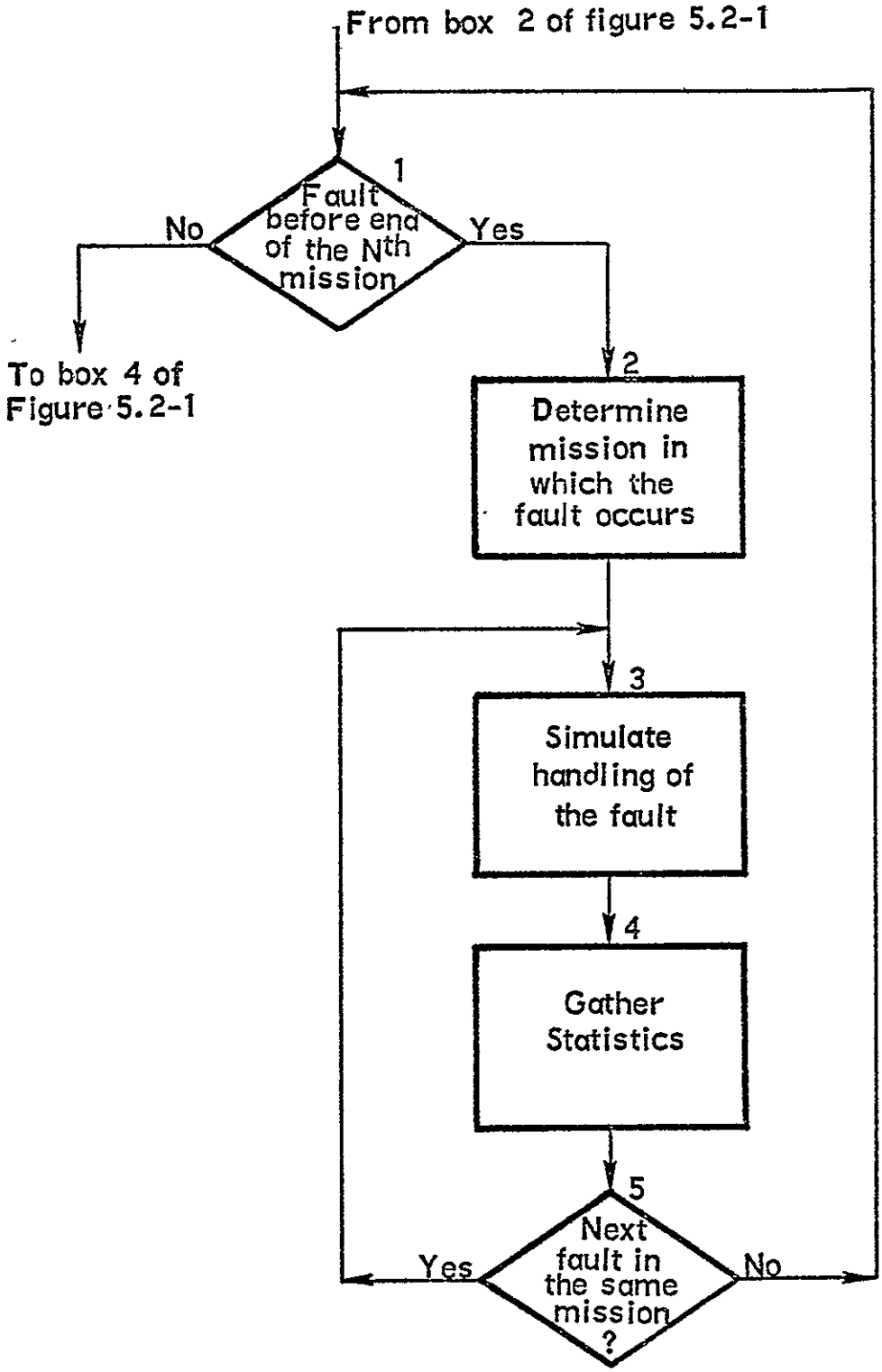


FIGURE 5.2-2 PRINCIPLES OF A FAULT DRIVEN SIMULATION (BOX 3 OF FIGURE 4)

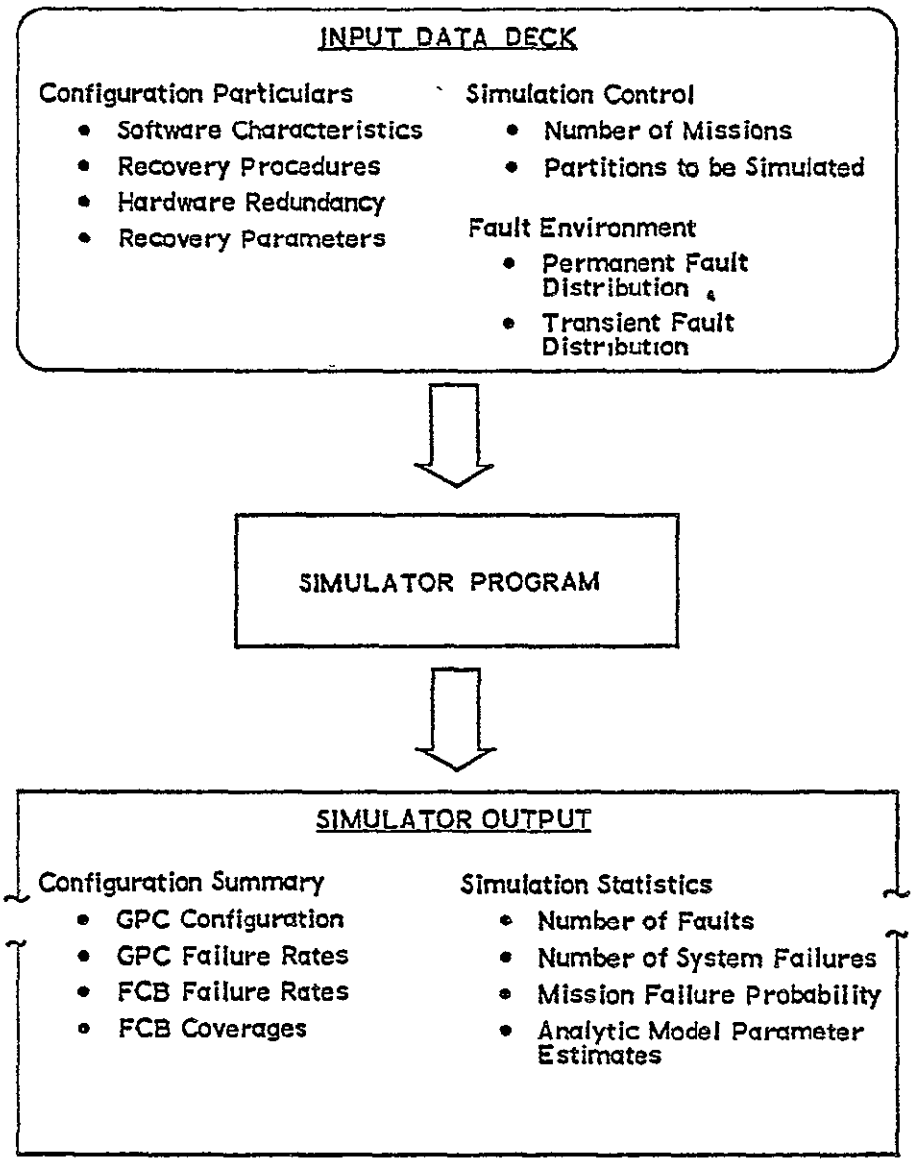
5.2.3 SIMULATOR UTILIZATION

The simulator provides the capability for estimating the fault handling abilities for a large number of configurations. In order to use the simulator, it is necessary to define the configuration and fault environment in detail, specify the simulator input parameters, set up a data deck, run the simulator program, and interpret the simulator results.

The system configuration is defined by the software characteristics, recovery procedures, hardware redundancy, and the recovery parameters. The fault environment is specified by the transient and permanent fault distribution functions. The software characteristics primarily affect parameters required for GPC simulation such as minor cycle duration, the major cycle duration, the time between inter-computer comparisons, the iteration period and the executive structure. The software characteristics indirectly affect other parameters such as recovery procedure performance parameters and fault coverage for FCB faults. The recovery procedures specify the method of transient recovery if any. Rollahead, rollback, memory copy, delay before reconfiguration and system restart are the possible recovery methods. The hardware redundancy is specified by the number of each type of system component, and their interconnections. Recovery parameters such as BITE detection probability and program survivability are determined by a detailed analysis of the system hardware. The fault environment is defined by the probability distribution functions of permanent faults, transient faults and transient fault durations. Permanent fault inter-arrival times are assumed to be exponentially distributed. Transient fault inter-arrival times can be exponentially distributed or burst distributed (see Section 5.3.3). It is necessary also to specify the parameters for the distributions (e.g. failure rates if the fault inter-arrivals are exponentially distributed). The input parameters are described in more detail in Section 5.5.1.

Once the input parameters are defined for the configuration, the simulation control parameters must be specified and the input deck must be set up. The parameter NMIS defines the number of missions to be simulated. The number of missions simulated has a bearing on the accuracy of the results; better accuracy is obtained by simulating a larger number of missions. The Flight Critical Bus partition and the GPC partition can be simulated together or separately because they are nearly independent. Thus if the effectiveness of several transient recovery procedures is being investigated it is only necessary to simulate the GPC partition in order to determine transient leakages. The input deck setup is given in Appendix B.

The simulator is then run and produces a configuration summary and some simulation statistics as output. The configuration summary includes a specification of the GPC configuration, the GPC fault environment, the FCB device failure rates and the FCB coverages. The simulation statistics includes the number of faults - both transient and permanent, the number of system failures, the number of "leaky" transients, and estimates of the mission failure probability and certain analytic model parameters. The simulator output is described in detail in Section 5.5.3.



5.3 SIMULATION OF THE GPCs

5.3.1 OVERALL GPC SIMULATOR STRUCTURE

The GPC simulator is organized as an "event driven," e.g., fault driven, simulation in order to minimize user computer costs.

The approach taken in the formulation of the GPC simulator is an extension of the approach described in KRUU 63. Formulating the simulator permits the computer system to be viewed as a finite state automaton. Thus, the system is described by the states it may assume and the possible transitions between states.

The computer system states are defined by two conditions. The first of these is the function being performed by the system. Examples of these are:

1. Normal Operation;
2. Recovery Operation,
3. Reduced Capability Operation,
4. System Restart; and
5. System Failure.

The second of the system-state defining conditions is that of the number of permanent faults that the simulated system has suffered during the particular simulated mission under consideration. Obviously, the system that has not yet encountered a fault will be in normal operation, while a system that has encountered faults may be in recovery operations, reduced capability operations, system restart, or may have failed.

Transitions between states in the simulated GPC system will be caused by either of two events. The first event that may cause a transition is the detection of a fault. For example, the first detection of a fault in the Shuttle GPC set causes a transition to the delay-reconfigurable state which simulates the FCOS transient-recovery method. Later detections of faults will cause a state transition in the simulated system. The second event, the completion of a recovery procedure, will definitely cause a transition to another state. What state is the destination of this transition depends on the type of recovery procedure attempted. For example, the successful completion of a normal recovery procedure when four GPCs are operating will return the simulator to the normal operations state. However, a recovery procedure that requires deactivation of one of three GPCs will cause the simulated system to transition to the duplex state.

An important aspect to be noted when considering the organization of the GPC simulator is that it is an "event driven" simulation. Thus, the initial state transition is only made when an event, in this case either a permanent or transient fault, occurs. Use of this type of structure provides a significant saving in computer time.

- System is Described by the States it May Assume and the Possible Transitions Between States
- States are Defined by:
  - The Function Performed by the System
  - The Number of Permanent Faults Assumed by the System
- Transitions are Caused by:
  - Detection of Faults
  - End of Recovery Procedure
- Resulting Simulation is Event Driven

5.3.2 STATE DIAGRAM

A state in the state diagram is defined by the number of properly-functioning computers and the action performed by the computer system at a given time.

Figure 5.3-1 presents the simplified state diagram of an adaptive NMR configuration that employs rollahead, rollback, and memory copy for transient-fault recovery. The algorithms involved in States I, II, III, and VII do not redundant states by maintaining a count in the simulation of the currently active computers.

NORMAL OPERATION (3 OR MORE UNITS)

In the normal operation state with three or more computer units, the outputs of the computers are periodically compared. Disagreement of one or more computers constitutes fault detection and requires exit from this state.

As long as two computers are fault-free, the rollahead recovery procedure is used and, if it is not successful, the memory copy. If all computers disagree at the same time, a system restart is initiated.

ROLLAHEAD (OR STATE VECTOR TRANSFER)

The rollahead state is entered to simulate the computer system's attempt to recover from a detected single fault. The state vector (consisting of program variables and all register contents) of one good computer is used to replace the non-agreeing computer's state vector. However, all transient failures are not corrected by this procedure since a bad instruction cannot be restored. The approach taken in the simulation is to provide for the specification of a rollahead success probability. This probability can be formally defined as:

$$P_{suc} = Pr\ [\text{fault is corrected fiven that a fault has occurred, has been detected, and its physical cause has disappeared when correction begins}]$$

An analysis, which gives consideration to the type of memory (e.g., 2 1/2D, 3D, DRO, NDRO, etc.) and the consequences of memory faults, will yield an estimate of the rollahead success probability (or program integrity).

MEMORY COPY

This recovery procedure is entered after a specified number of rollaheads have been completed unsuccessfully. The memory contents of one good

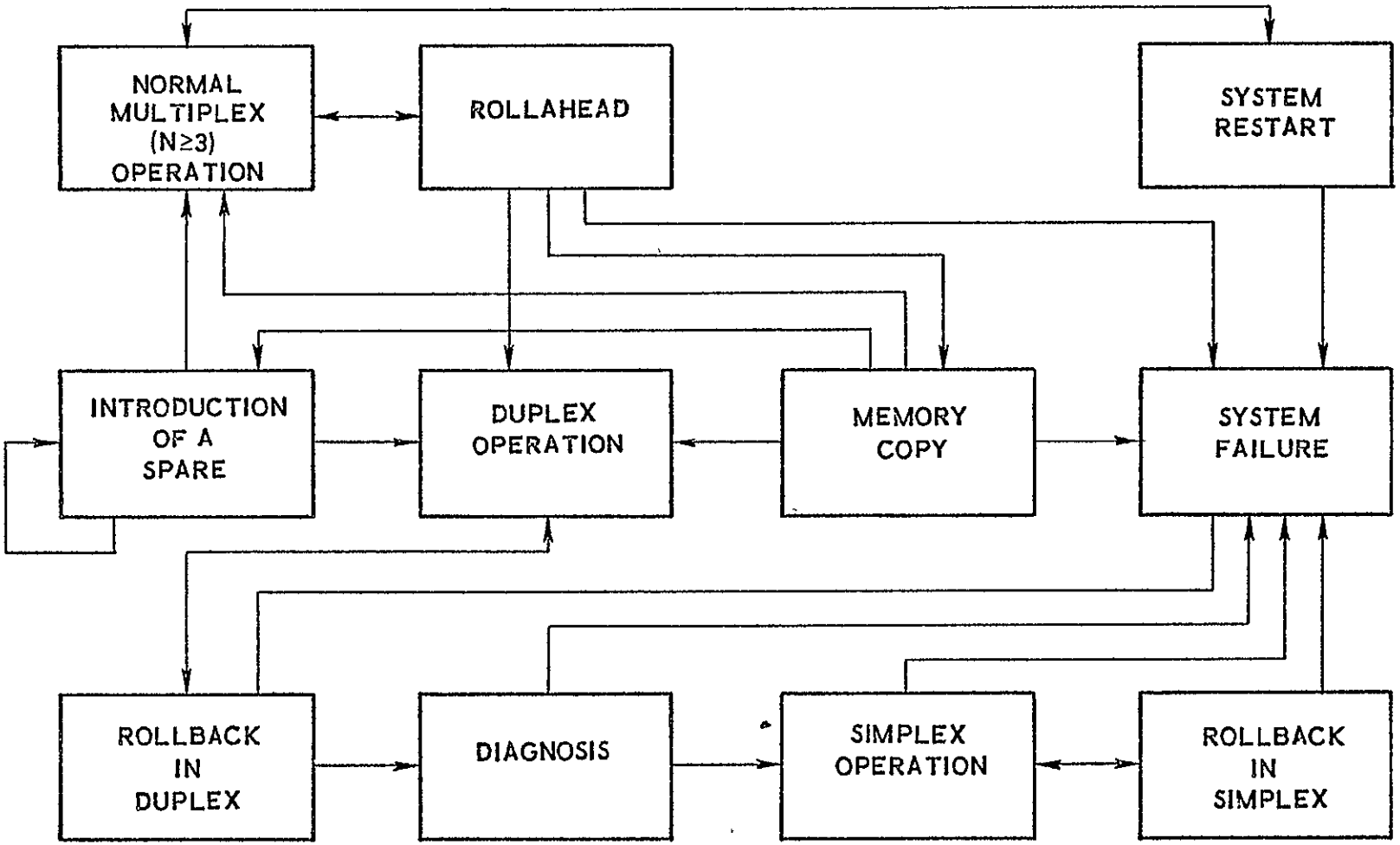


FIGURE 5.3-1 SIMULATOR STATE DIAGRAM

memory are transferred into the faulty memory. In order to avoid interruption of computation, the transfer is effected on the basis of cycle stealing. It ends with the updating of the state vector of the faulty computer.

Since, during a memory copy, normal application routines continue, it is possible that a new fault shows up. The following (conservative) assumption has been made in order to simplify the simulation. Upon detection of a second fault during a memory copy, the memory copy procedure is abandoned and the computer for which this memory copy was intended is discarded.

It is assumed that memory copy provides recovery from transient faults which have disappeared when the memory copy began with a probability equal to the memory copy efficacy.

SYSTEM RESTART

The system restart state is entered when all computers disagree upon comparison. The recovery procedure from this state may consist of a memory verification. Relevant memory locations are read, voted upon, and restored. Extensive diagnosis may also be run. Finally, if a backup memory is available, reloading may be possible. Then the application program is reinitiated from the restart point.

After a successful system restart, the system returns to the normal operation state. However, since all computers stop their normal computation during a system restart, this recovery procedure is time critical.

Note that in a benign fault environment, the probability of having a system restart is quite small ($\simeq 1$ for 1 million faults). However, system restart is necessary if the fault environment is so harsh that bursts of faults can hit several computers at a time or if the probability of a short power failure is not negligible.

INTRODUCTION OF A SPARE

If a spare is available, it should be activated once a permanent fault has been recognized. As part of the activation process, the spare is checked and conditioned by one of the good computers. In the situation depicted in the state diagram of Figure 5.3-1 spares are not available for the duplex and simplex simulation. This is thought to be compatible with the expected applications.

NORMAL OPERATION (2 UNITS)

The normal operation (2 units) state is entered upon the determination that a permanent fault exists in one of the three computers on the computer system. This state is quite similar to the normal operation (N units) state, except that the only available recovery procedure is program rollback.

ROLLBACK

The rollback state is entered upon the detection of a fault when the computer system is in the normal operation (2 units) state. Rollback is the term used to describe repetition of the program segment executed just prior to the detected output disagreement. The state vector at the beginning of each program segment is maintained in order that the rollback procedure may be accomplished.

After the program segment has been repeated, the outputs of the two computers are compared; if the correction is successful, the computer system switches back to the normal operation (2 units) state. If the output differs, the system rolls back again; this unsuccessful recovery process continues a predetermined number of times before changing the computer system state to diagnosis.

Since both of the active computers remaining in the computer system must stop their normal computations during a rollback, this computer recovery procedure may be time-critical. However, if comparisons are frequent enough, a rollback should not last more than a few milliseconds.

DIAGNOSIS

In triplex, voting provides a very easy and efficient way of isolating the faulty unit. Unfortunately, a disagreement upon comparison in duplex does not indicate which of the computers produced the wrong value. That is why the main recovery procedure in duplex is the rollback since there is no transfer of information from the good to the bad computer for such a procedure. But, if the rollback does not succeed, the bad computer must be isolated. For that purpose, self-tests are run. If they are successful, the faulty computer is isolated and the system switches to simplex. If unsuccessful, the system is unable to decide which computer is faulty and the system fails. Diagnosis programs are obviously time critical. Note that it would be possible to include a memory copy which would take place once a diagnosis had been successful: the

memory of the good computer would be copies into the bad one. However, this improvement is not so good as it would seem since many transients cannot be detected through diagnosis.

NORMAL OPERATION (SIMPLEX)

In simplex operation, comparison is no longer available for detection of faults. We must rely mostly on the RETs to detect faults. CPU transients are difficult to detect. Some may be caught through go/no-go counters and storage protection. Memory faults are easier to detect. Parity check is especially useful. When a fault is detected, a rollback is initiated. If the fault is not detected, a failure occurs.

ROLLBACK IN SIMPLEX

This is the same procedure used in duplex. Since it is the only recovery algorithm available in simplex, it is repeated as long as it is not successful. If recovery from the fault cannot be effected, a system failure will occur when the system has been down too long.

SYSTEM FAILURE

The system failure state is entered with the system is unable to run properly and longer or when computational requirements have not been met for too long a period of time. Upon recognition of the condition of a system failure, the DRIVER program discontinues the simulation of a mission.

Causes of failures are:

1. Excessive time in rollahead, memory copy, or rollback: It should not happen since the system must be designed so that a recovery procedure does not endanger it. However, it might happen that the continuous repetition of such procedures be fatal for the successful completion of the mission.
2. An overly-long system restart: A system restart is a very rarely called procedure. But it is long (a few seconds), and may not always be tolerable.
3. Diagnosis incomplete when available recovery time expries: Normally, diagnosis follows rollback. It is possible that these two recovery procedures sometimes take too long.

4. Undetected faults in simplex.

5. A too long rollback in simplex: This happens when a permanent occurs or when a non-recoverable transient occurs.

6. EEM failures: In the case of non-dedicated EEMs, the system fails when all EEMs fail or when all but one fail and the computers are unable to decide which is the good EEM.

7. Bus failures: The system fails when all buses fail or when all but one fail and the computers are unable to decide which is the good bus.

8. Actuator/sensor failures.

5.3.3 FAULT GENERATION

A flexible approach to the generation of faults was chosen for use in the RCS simulator

A major portion of the simulator is dedicated to the generation of faults according to mathematical algorithms which describe the occurrence of faults in the various components of the computer system. Two approaches to handling this problem were considered:

1. Generation of one fault at a time.
2. Generation of a fault table describing the faults which occur in the computer system between 0 and a time T.

The first approach is suitable if we consider only single faults and if we simply describe fault occurrences within the computer system, e.g., the fault-arrival rate in the system is λ and the probability that a fault is in the i^{th} part of the computer system is P_i. This procedure is described in LYON 62.

Since we must deal with transient failures also, we want to know how the computer system behaves in case of multiple faults. Furthermore, if the faults do not occur according to a Poisson law in all modules (burst of transient failures for example), the method described in LYON 62 is not readily applicable.

A more efficient and more general approach is to generate a fault table prior to simulation. This also makes the simulation program more functionally modular since, once the simulation has begun, we have only to scan the fault-table to determine when and where the next fault occurs.

PARAMETERS

The parameters necessary to generate the fault table for a simulator run are a part of the parameters of simulation which are input by the simulator user for each simulator run.

DESCRIPTION OF THE COMPUTER SYSTEM

The computer system to be simulated is composed of n identical computers, each composed of m modules.

DESCRIPTION OF THE FAULT DISTRIBUTIONS

For each of the m modules, the distribution functions to be used in generation of both permanent and transient faults must be indicated by the simulator user. Specific subroutines for the chosen distribution functions are then called and the parameters of the distribution are passed to these subroutines.

For permanent faults, only the Poisson distributions have been implemented. This is generally considered in the literature to be most realistic.

For transient faults, Poisson and burst distributions have been considered. Poisson distributions are considered because of their tractability and acceptance for the permanent fault case. Burst distributions are thought to be important because many transients likely are caused by components working near the limits of their tolerance specifications. As long as the conditions do not improve, faults will occur often in these components. A burst of transients is defined by its duration and the rate of transient occurrence during the burst. Bursts occur according to the burst rate.

DESCRIPTION OF THE FAULT DURATION

For each of the m modules, the distribution function of the transient failure durations to be used by the simulator programs must be indicated by the simulator user. Specific subroutines for the chosen distribution functions are called by the Driver and the subroutines receive the parameters of the distributions.

At the present time, the uniform and the exponential distributions have been implemented.

1. Uniform Distribution -- The transient failure duration is uniformly distributed between a minimum and a maximum duration.
2. Exponential Distribution -- The transient failure duration is exponentially distributed. The mean duration is $1/\gamma$.

DESCRIPTION OF THE FAULT TABLE

The fault table consists of 300 records ordered according to the occurrence time of each fault. This table can contain up to 150 permanent faults and 150 transient faults. It has the following record format:

Occurrence Time	Duration	Module	Computer

Permanent failures are identified by a duration longer than the mission time.

GENERAL ORGANIZATION OF THE FAULT GENERATOR

The first step consists of generating a table of permanent failures and a table of transient failures for each module in the computer system. Then these tables are merged into one sequentially-ordered (master) fault table. The general organization of the fault generator is presented in Figure 5.3-2.

DETERMINATION OF THE OCCURRENCE TIME OF THE FAULT ACCORDING TO A POISSON DISTRIBUTION FUNCTION

Faults occurring by a Poisson distribution process have a probability that one fault occurs during a small interval of time, dt, as follows:

$P_1 = \lambda dt$. (See PARZ 60).

The probability of no faults, P_0, occurring during the time interval dt is, $P_0 = 1-\lambda dt$, and the probability of more than one fault occurring is 0.

A Poisson distribution process has two very important properties:

1. It is memoryless: This means that the probability of a fault occurring between times t and t+dt is independent of fault occurrences before time t.

2. The probability density function for the random variable, T_τ, i.e., the interarrival time between two consecutive faults, is

$$f_{T_\tau}(t) = \lambda e^{-\lambda t}$$

Thus the probability distribution function of T_τ is:

$$P[T_\tau \leq t] = \int_0^t f_{T_\tau}(u)\, du$$

$$= 1 - e^{-\lambda t}$$

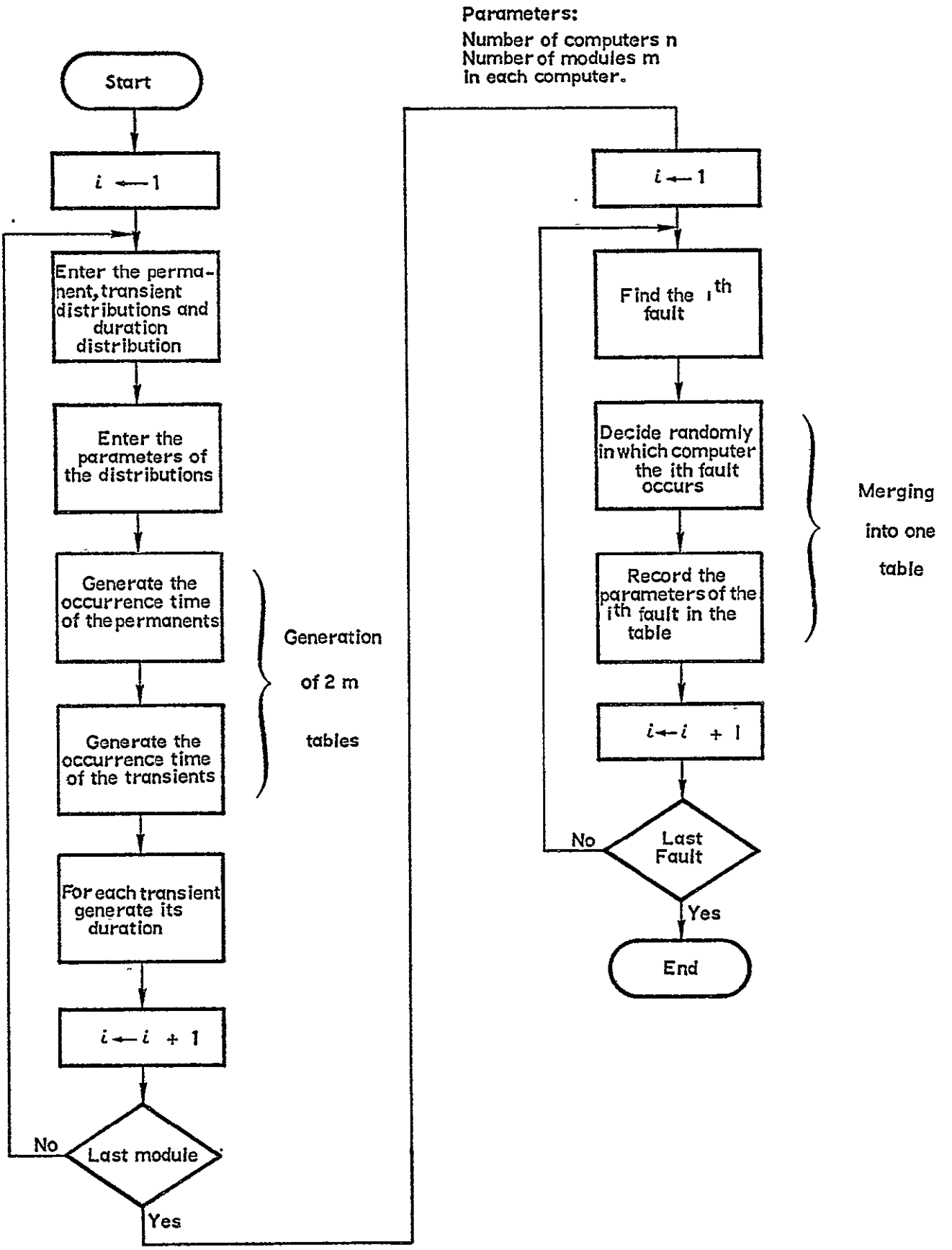


FIGURE 5.3-2 GENERAL ORGANIZATION OF THE FAULT GENERATOR

Thus the probability of having no fault at time t is:

$$R(t) = e^{-\lambda t}$$

A difficulty arises at this point since the random number generator (function) available in the CYBERNET system produces outputs which are uniformly distributed on the interval $0 \leq U \leq 1$. The outputs of this generator can be converted using the approach described below. (HILL 70, SHRE 66).

We are concerned with the random variable T_τ, the interarrival time between faults, whose distribution function is given above as

$$P[T_\tau \leq t] = 1 - e^{-\lambda t}$$

For the purposes of the simulation we wish to obtain values of t. We now note two important facts. First, $0 \leq P \leq 1$. Second, by algebraic manipulation it is possible to solve for t, e.g.:

$$t = -\frac{1}{\lambda} \ln (1-P)$$

Thus, for any value of P in the valid range, a value of t can be calculated. By generating values of P using the random number generator, which produces uniformly distributed numbers between zero and one, t can then be calculated.

A more formal description of the process follows. Using the random number generator which gives a number U uniformly distributed on the interval $0 \leq U < 1$, we have to compute T_τ which is exponentially distributed. That means that we have to find a function f(U) such that:

$$T_\tau = f(U)$$

and $P[U \leq u] = u$ (uniform distribution) (if $0 \leq u < 1$) $\qquad P[T_\tau < t] = 1-e^{-\lambda t}$

If $T_\tau = f(U)$, we can define the inverse function $g(T_\tau)$ such that $U = g(T_\tau)$.

Thus, we have:

$$P[T_\tau \leq t] = 1-e^{-\lambda t}$$

$$= P[f(U) \leq t]$$

$$= P[U \leq g(t)]$$

$$= g(t)$$

The last equation is true since U is uniformly distributed on the interval, $0 \leq U < 1$. Thus we know that the unknown function f(U) is the inverse of the function $g(t) = 1-e^{-\lambda t}$.

Hence:

$$u = g(t) = 1-e^{-\lambda t}$$

$$t = -\frac{1}{\lambda} \ln (1-u) = f(u)$$

Since we have just found the function f, we can write

$$T_\tau = -\frac{1}{\lambda} \ln (1-U)$$

But we can have a simpler expression: U is uniformly distributed on the interval, $0 \leq U < 1$. Hence 1-U is also uniformly distributed on the same interval. This implies that the distribution of T_τ does not change if we replace 1-U by U.

Finally, we have shown that if U is uniformly distributed on $0 \leq U < 1$, then $T_\tau = \frac{1}{\lambda} \ln U$ is exponentially distributed, the parameter of the distribution being λ.

Using the random number generator provided by the CYBERNET system, we determine the different interarrival times and thus the occurrence times. The flowchart of the generation of the occurrence times of the faults in one module is presented in Figure 5.3-3.

DETERMINATION OF THE DURATION

As stated earlier, both exponential and uniform distributions of transient fault duration are available in the simulator. If the transient duration is exponentially distributed (parameter γ), we determine a duration D_T for each transient:

$D_T = -\frac{1}{\gamma} \ln U$ using the same general procedure described for the occurence time. If the duration is uniformly distributed on $0 < D_T < D_{max}$, the duration D_T is $D_T = D_{max} \times U$.

DETERMINATION OF THE OCCURRENCE TIME OF THE FAULTS ACCORDING TO A BURST DISTRIBUTION FUNCTION

The occurrence time and duration of the bursts is determined as described above for faults having a Poisson distribution function. Then,

for each burst, the occurrence time and duration of the transients are determined.

SUMMARY OF FAULT-GENERATION POSSIBILITIES

From the above discussion, it can be seen that there are a number of fault-generation possibilities that can be used in the simulator. With respect to permanent faults, the standard fault generator is one that generates faults according to a Poisson distribution function. However, as a result of the presence of the uniform distribution random number generator, it is possible to use other distributions that are expressible analytically. For transient faults of the non-burst variety, the occurrence rate and the duration are modeled and each of these may conform to either a Poisson or another distribution. Burst faults are characterized by four parameters, i.e., the burst-packet occurrence rate, the burst-packet duration, the fault occurrence rate within the burst packet, and the duration of the individual faults. Each of these rate durations can be modeled using either Poisson or other distributions.

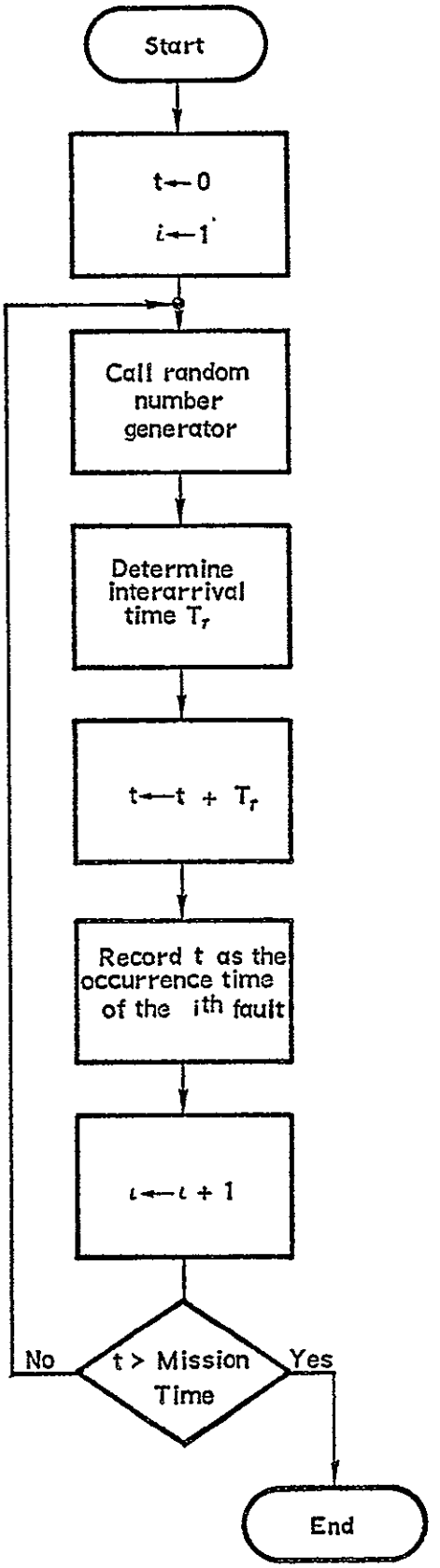


FIGURE 5.3-3 GENERATION OF THE OCCURRENCE OF THE FAULTS IN ONE MODULE (POISSON DISTRIBUTION)

5.4 SIMULATION OF FLIGHT-CRITICAL BUS SUBSYSTEM

5.4.1 GLOBAL APPROACH TO FCB MODELING

For survivability assessment purposes, the Shuttle Data Processing Subsystem was partitioned into seven independent equipment groups, as follows: the five general-purpose computers (GPC); the flight-critical buses and connected equipment (FCB); the two mass memory units and their buses (MM); the display equipment and their buses (DIS); the payload operations equipment and buses (PLO); the launch related equipment and buses (LE); and the flight instruments and buses (FI).* The input-output partition (I-O) includes all of the above equipment groups except the GPC partition.

The diagram on the opposite page shows the layout of the flight critical bus partition which is the most complicated input-output equipment group. The eight flight-critical buses, FC1 - FC8, are interfaced with all GPCs. Each dedicated display unit (DDU) is interfaced with three buses by means of three redundant ports. The flight-forward MDMs are each interfaced with two buses by means of a primary port and a secondary port. If the electronics associated with a primary port fails, the backup port is switched in. Each interface unit (MDM or DDU) controls several dedicated and/or non-dedicated devices (non-dedicated devices are shaded and can be accessed through more than one MDM). These devices are redundant (e.g., ACCEL1, ACCEL2, and ACCEL3 perform identical functions), thus one of them can fail without causing a system failure.

The I-O partition simulation modeling is different from the GPC partition simulation modeling, in that the state of the I-O partition is represented by a set of tables rather than a procedure as for the GPC partition. This method was chosen because the I-O partition requires many more states than the GPC partition, and the simulation of a particular I-O state is much simpler than the simulation of a GPC state since no software considerations need be taken into account.

The behavior of each equipment group in the I-O partition is represented by several tables and a procedures. The tables define the current state of the system; i.e., the partition status, the device interconnections, and the partition's recovery capabilities. The procedures define the fault-induced system action, the resulting table modifications (i.e., state transition), and the

*See Section 4.1 for an explanation of the DPS partitioning.

successfulness of the recovery. Both the built-in test equipment and the redundancy management software are factored into the implementation of these procedures, since they define fault detection, isolation, and recovery success probabilities. The next topic discusses the simulator representation of the flight critical bus partition.

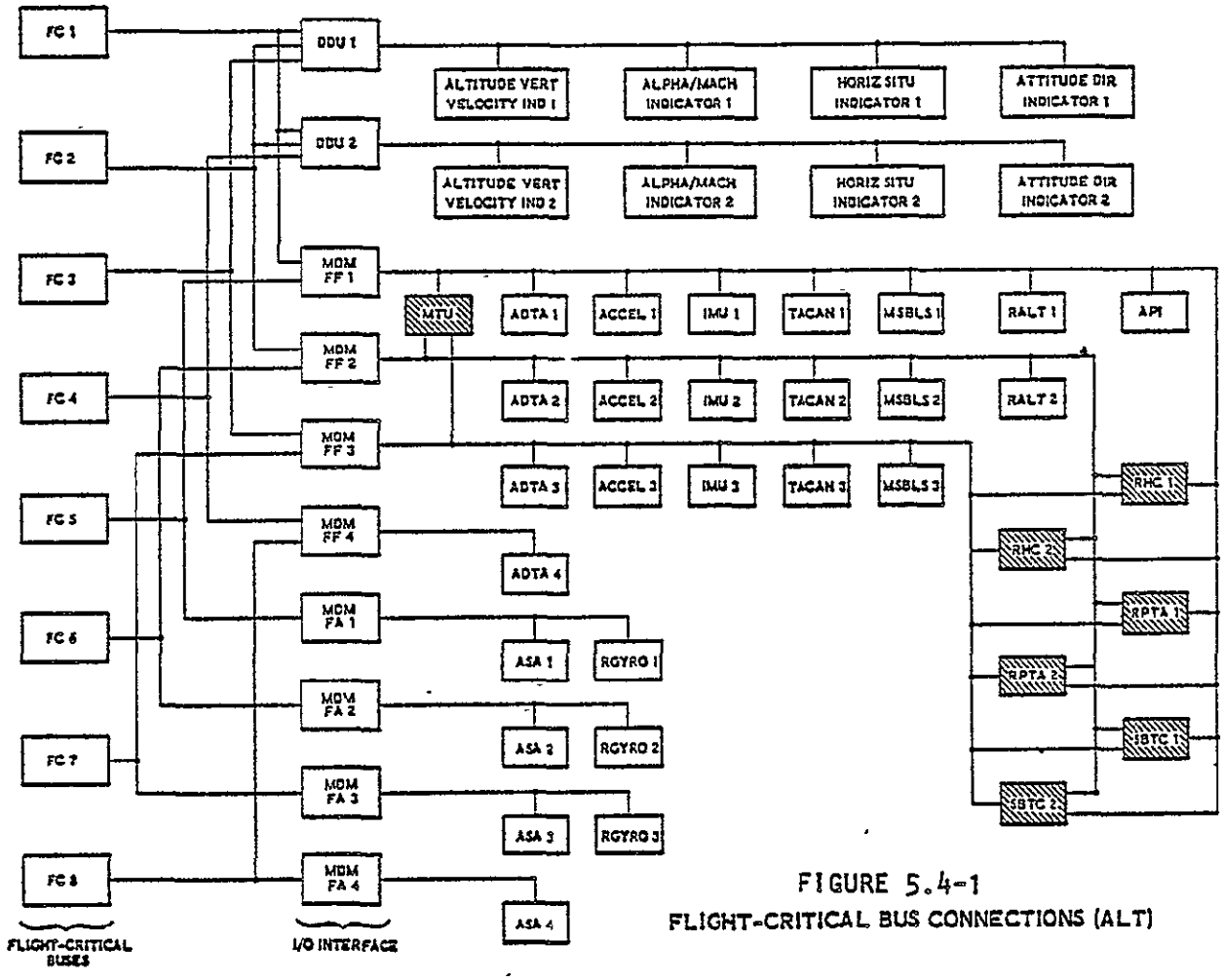


FIGURE 5.4-1
FLIGHT-CRITICAL BUS CONNECTIONS (ALT)

5.4.2 FCB SUBSYSTEM STATUS REPRESENTATION

The status of the flight-critical-bus partition is represented in memory by a set of tables like the ones on the facing page. Table 5.4-I indicates the interconnection between the flight-critical buses (FC1 - FC8) and the IUs (interface units, i.e., MDMs and DDUs). Table 5.4-II reflects the relationship between the flight-forward MDMs (MDMs FF1 - FF4) and the dedicated sensors and actuators. Additional tables relate the MDMs and DDUs to the other devices. A procedure is invoked to determine and record the effects of a fault in the flight-critical bus partition on the system.

The interface between the flight-critical buses and the IUs is reflected by Table 5.4-I on the facing page. Each row corresponds to a flight-critical bus and each column corresponds to an IU. An element that is indexed by a particular bus and IU (row and column) is assigned to a number according to the following scheme:

0 — The bus does not have a functional interface with the IU.

1 — The bus has an active interface with the IU.

2 — The bus has a functional, but inactive, interface with the IU (i.e., this represents a secondary port).

Thus from Table 5.4-I, it can be inferred that MDM FF1 is interfaced with flight-critical buses FC1 and FC5. FC1 is connected to the primary (active) port of MDM FF1, and FC5 is connected to the secondary port. Note that each DDU has three active ports. Here it is assumed that display information is transmitted on buses FC1 - FC4, and the actual bus used by a DDU is selected by a manual switch on its control panel.

The interface between MDMs FF1 - FF4 and the dedicated sensors and actuators they control is indicated by Table 5.4-II. Each row corresponds to a flight-forward MDM, and each column corresponds to devices of a particular type. An element corresponding to a particular MDM and type of device has a value of "0" or "1" which indicate:

0 — A functioning device of this type is not associated with the MDM.

1 — A functioning device of this type is connected to the MDM.

Thus Table 5.4-II indicates three accelerometers with ACCEL1 interfaced to MDM FF1, ACCEL2 interfaced to MDM FF2 and ACCEL3 interfaced to MDM FF3.

	DDU1	DDU2	FF1	FF2	FF3	FF4	FA1	FA2	FA3	FA4
FC1	1	1	1	0	0	0	0	0	0	0
FC2	1	1	0	1	0	0	0	0	0	0
FC3	1	0	0	0	1	0	0	0	0	0
FC4	0	1	0	0	0	1	0	0	0	0
FC5	0	0	2	0	0	0	1	0	0	0
FC6	0	0	0	2	0	0	0	1	0	0
FC7	0	0	0	0	2	0	0	0	1	0
FC8	0	0	0	0	0	2	0	0	0	1

TABLE 5.4-I Bus - BTU Interconnection Matrix

	ADTA1	ACCEL	IMU	TACAN	MSBLS	RALT
FF1	1	1	1	1	1	1
FF2	1	1	1	1	1	1
FF3	1	1	1	1	1	0
FF4	1	0	0	0	0	0

TABLE 5.4-II MDM - Device Interconnection Matrix

5.4.3 ORGANIZATION OF FCB SIMULATION PROGRAM

The effects of faults occurring in the flight critical bus partition is simulated by the subroutine FCBFLT, which is flowcharted in Figure 5.4-2. This routine first determines the fault location, and then calls the appropriate fault simulation routine. If the fault results in a safety-critical failure, then system failure is indicated. Otherwise, a status vector is set to indicate the loss of any functions that have an effect on GPC performance (e.g., the MTU). Control is then passed back to the calling program, FIFAU.

The six FCB fault simulation routines are: BUSFLT for simulating the occurrence of a fault on a flight-critical bus, MDMFLT for simulating faults occurring in the flight-critical bus terminal units, and DDUFLT, DFFFLT, NFFFLT, and DFAFLT for simulating faults occurring in the device interfaces with the bus terminal units. Each routine has similar program logic. The status of the unit in which the simulated fault occurred is first checked. If the unit has already failed, the fault is ignored and control passes back to FCBFLT. Otherwise, the fault counter is incremented and control is passed the appropriate program segment determined by the fault type.

If the fault is transient, the transient-fault counters are first incremented and then transient recovery is simulated. If the fault corrupts data and is undetected, it is assumed critical. If the fault disappears within a certain time period (the time required for transient recovery, i.e., a RETRY) and causes no permanent damage, transient recovery is assumed successful and control is returned to FCBFLT. Otherwise, the fault is handled as a permanent (it is assumed that FCOS mistakes the transient for a permanent and acts accordingly).

Permanent faults result in replacement, or deletion with redundancy masking of the fault unit. If the unit is removed, all devices that depend upon it are also removed. Thus, if one of the flight critical buses permanently fails, it is removed from the system (all I/O transactions requiring it are terminated). All bus terminal units using the faulty bus, switch to their backup ports interfaced with other buses. If no backup ports are available to a BTU (Bus Terminal Unit), it is indicated as failed and thus removed from the system. Thus, all devices connected to it can no longer function, and must be removed from the system. If the status now indicates that a necessary device is no longer available, a flight critical failure is indicated.

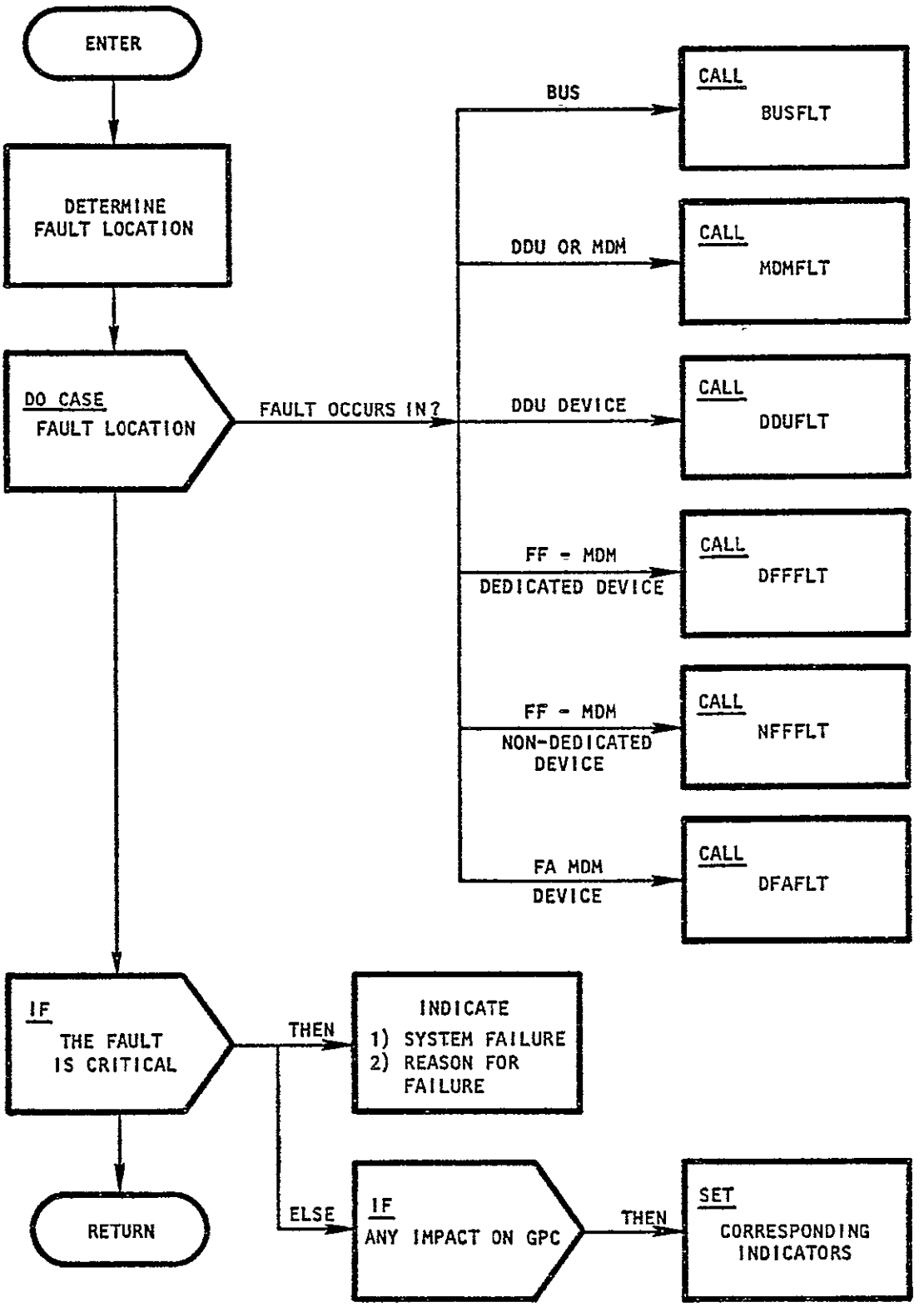


FIGURE 5.4-2 STRUCTURE OF FCBFLT SUBROUTINE

5.4.4 INTEGRATING FCB SIMULATION SUBROUTINES WITH THE MAIN PROGRAM

The Input-Output fault simulation subroutines are integrated with the GPC simulation routines by means of the subroutine FIFAU, which is invoked for every simulated fault to determine how it is to be simulated. FIFAU distinguishes between three classes of faults. Those occurring in a GPC's CPU or Memory are simulated by the GPC state simulation subroutines. Faults occurring in one of the I/O equipment groups are simulated by the I/O simulation subroutines. Those faults appearing in the GPC's IOP are simulated by the GPC state-simulation routines or the I/O simulation-routines, or both depending on its impact. Most IOP faults result in a GPC failure, because the IOP is needed as an interface to the I/O network; however, it is possible that an IOP fault could also disable a bus (e.g., a fault occurring in an IOP's BCE could appear to be a bus fault, to FCOS, thereby resulting in bus replacement, effectively disabling the bus).

The overall control sequence for the subroutine FIFAU is shown in Figure 5.4-3. FIFAU first determines where the simulated fault occurs and jumps to the corresponding program segment (illustrated by DO CASE statement in Box 1 of the flowchart). If the simulated fault occurs in the CPU or Memory, the program sequence follows the CPU/memory branch (branch 2); if the fault occurs in the IOP, control follows branch 3; and if the fault occurs in the I/O network, control follows branch 4 and executes the I/O simulation routines. Upon completion of the program segment, control returns to the statement following the DO CASE, and then returns to the calling program with two parameters IN and NEXT. IN indicates to the calling program if it is necessary to simulate GPC recovery for that fault. NEXT is set if a system failure has occurred as a result of an I/O fault.

The CPU/Memory program segment first determines if the unit in which the simulated fault occurs has already failed. If it hasn't, then IN is set to indicate that simulation of GPC recovery is necessary, and control is returned to the calling program. If the GPC has already failed, the fault is ignored by setting IN to indicate that no GPC recovery-simulation is necessary.

The IOP program segment determines the impact of the IOP fault on the bus and GPC. If the bus is impacted, a routine is invoked to simulate recovery, and then status indicators are set to indicate the resulting system status. If the CPU's capability for receiving correct data is affected, then IN is set to indicate that GPC recovery is still necessary, otherwise, the bus recovery

routine (e.g., switching the bus connected to a faulty BCE) is assumed to have corrected the fault, and IN is set to indicate that further processing for this fault is unnecessary. If access to critical devices were lost as a result of bus replacement, NEXT is set to indicate the occurrence of a safety critical failure.

Program segment 4 first determines which equipment group the fault occurs in, and them invokes the appropriate simulation routine (e.g., if the fault occurs in the flight critical bus partition, the routine-FCBFLT is invoked). If a safety critical function was lost, NEXT is set to indicate such, otherwise, IN is set to indicate that no further simulation is necessary for this fault.

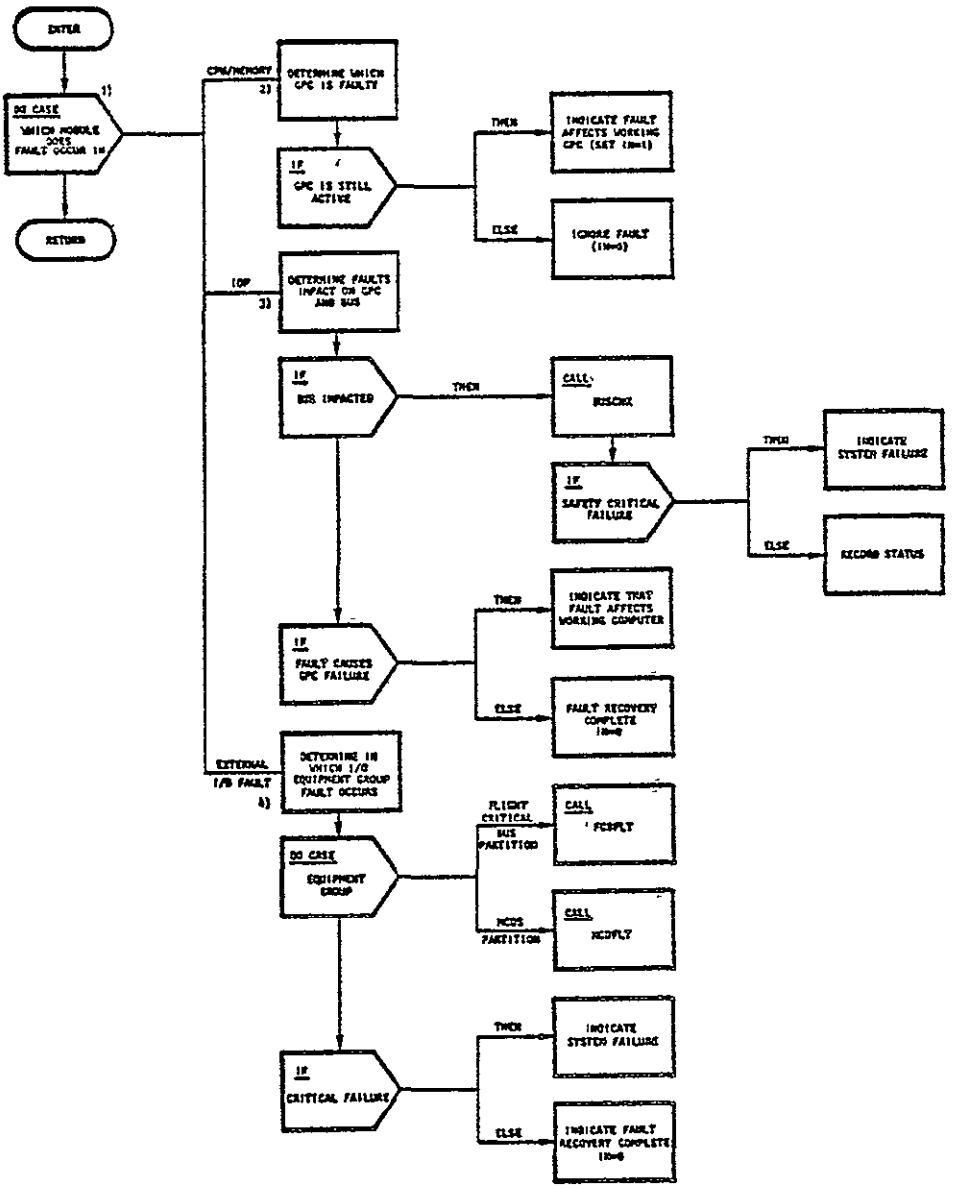


FIGURE 5.4-3 FIFAU OVERALL CONTROL SEQUENCE

5.5 SIMULATOR UTILIZATION

5.5.1 SIMULATOR INPUTS

The inputs required by the simulator are summarized in Tables 5.5-I and 5.5-II. The detailed simulator input deck set-up is given in Appendix B.1. The use of some of these inputs is discussed below.

The detection probabilities are the probabilities that a computer detects its own faults (except through diagnosis). This is not significant for N-M-R configurations ($N \geq 3$) since all faults are detected and located through voting or comparison. However, these probabilities become critical in duplex and simplex. In duplex, faults are detected through comparisons. However, BITE or self-test is needed to isolate the faulty computer. In simplex, BITE is necessary, since it provides the only means for detecting transient faults.

For simplex operation the detection probability of CPU faults is low. Faults in the CPU usually cause only a wrong output which will not be detected by BITE. However some will be detected. Those are the ones which cause a forbidden address to be computed or those which modify the computing sequence in such a manner that a go/no-go counter detects them. IBM estimates this detection probability to be about 35%.

The main technique to detect a memory fault is parity encoding. When it exists, the probability of detecting a memory fault is usually better than 80%. When it does not exist, this probability is quite small.

Self-test programs (diagnosis) are run in a duplex system where a fault has been detected but not isolated. Note that if the fault is transient, the self-test will probably not diagnose it, since it usually dissipates before the test is run.

If the configuration includes some additional hardware for the Input-Output Processor, the consequence of faults in this hardware has to be assessed. We partitioned the configurations in two classes. In the first class (dedicated IOPs), we assume that a fault in the IOP is equivalent to a fault in the computer and sometimes on the corresponding bus. In the second one (non-dedicated IOPs), we assume that IOPs are independent from the computers. The system can work as long as one computer and one IOP are good. Note that the dedicated case includes software TMR.

In the present simulator, the recovery procedure for a NMR system is the state vector transfer. Memory copy is optional.

TABLE 5.5-I · REQUIRED SIMULATOR INPUTS - GPC PARTITION

NUMBER OF SIMULATED MISSIONS

MISSION DEPENDENT PARAMETER

- Mission Time

MACHINE DEPENDENT PARAMETERS

- Permanent Failure Rates
- BITE Detection Probability of a CPU Fault
- BITE Detection Probability of a Memory Fault
- Self-Test Program Efficiency
- Self-Test Program Duration

CONFIGURATION-DEPENDENT PARAMETERS

- Number of Computers
- Number of Spares
- Dedicated/Non-Dedicated IOPs (Input-Output Processor)
- Probability that an IOP Fault Hits the Bus
- Number of Non-Dedicated IOPs
- Applicable Recovery Algorithms
- Recovery Algorithm Characteristics
- Duration
- Unacceptable Recurrence Interval
- Maximum Number of Rollbacks
- Program Integrity
- Memory-Copy Efficacy

SCHEDULING PARAMETERS

- Iteration Period
- Time Between Comparisons
- Major and Minor Cycle Durations
- Asynchronous/Sunchronous Mechanism

ENVIRONMENT DEPENDENT PARAMETERS

- Transient Failure Rates
- Transient Failure Duration

Once a recovery procedure has failed for a certain fault, it is useless to attempt to recover through the same procedure. Some other one has to be chosen. If after completion of a recovery procedure, a fault recurs in the same computer after a time less than the unacceptable recurrence interval, the system decides that the recovery procedure was unsuccessful and attempts something else. Usually, the recurrence intervals will be chosen equal to the duration of one major cycle. The rationale is that the memory is thoroughly exercised in one major cycle.

The Program Integrity is listed with the other recovery algorithm characteristics because a transient recovery algorithm not involving memory refresh cannot succeed when there is a program memory damage. Program integrity is strongly linked to the type of memory: an NDRO memory is much better in this respect than a DRO memory. The fact that there is no need to restore the information makes it very unlikely that a transient fault damages instructions or constants. In addition, in most NDRO applications, the write voltage for the program memory is disabled except when altering the program under AGE control.

The memory copy-efficacy is the probability that a memory copy corrects a transient fault. The only reason why it should not succeed is that the transient had hit the little (micro) program initiating the memory copy. This is very unlikely since this program should reside in a read only memory or microstore.

Table 5.5-II lists the required simulator inputs for the FCB partition. The redundancy and interconnections between FCB components are specified by five arrays. In general, an array element equal to one indicates that a connection between the devices, indicated by the row and column indices, exist, and a zero indicates the opposite. These matrices are described in more detail in Section 5.4. Device names, which are used for identifying components on the simulator listings, are specified in the input deck to allow more flexibility. Because of the large number of devices on the FCB bus, recovery characteristics are specified by transient fault detectabilities, transient leakages and coverages, rather than by specific recovery procedures. Eighty-nine cards are needed to specify the FCB configuration and failure rates.

TABLE 5.5-II REQUIRED SIMULATOR INPUTS - FCB PARTITION

CONFIGURATION-DEPENDENT PARAMETERS

- Number of I/O Devices
- Redundancy of I/O Devices
- Interconnections Between I/O Devices

DEVICE DEPENDENT PARAMETERS

- Device Identification Names
- Transient Fault Detectabilities
- Transient Fault Leakages
- Fault Coverages

FAULT ENVIRONMENT

- Permanent Failure Rates
- Transient Failure Rates

5.5.2 OBTAINING SIMULATOR INPUT PARAMETERS

An important point in the application of CAST to the shuttle data processing subsystem is the determination of simulator input parameters. There are several methods for obtaining them if their values are not obvious: Failure rates and built in test detection probabilities are usually obtained from the manufacturer. Parameters affecting transient fault recovery such as the PROGRAM INTEGRITY or transient leakages can be determined by engineering analysis or by logic level simulation.

Parameters that couldn't be obtained from the manufacturers were estimated by an engineering analysis. One of the required simulator inputs is called program integrity (PI). This simulator input is the probability that a transient fault in the GPC memory does not alter a program word.

We use a "top-down" approach by subdividing the GPC memory into functional components and then in turn further partitioning these functional components. For each transient failure mode within a component we determine whether memory will

- Always be corrupted,
- Be corrupted only if the component is used, or
- Never be corrupted.

The expression for the program integrity can be written as one minus the probability that a transient fault alters a program word. Thus PI is written as

$$PI = 1 - \left(\sum_i n_i \sum_j \beta_{ij}\tau_{ij}\right) \Big/ \left(\sum_i n_i \sum_j \tau_{ij}\right)$$

where: τ_{ij} is the rate of occurrence of transient failure mode j in component i,

β_{ij} is the probability that transient failure mode j in component i corrupts memory, and

n_i is the number of components of type i.

The first partitioning of a 16K - 2 1/2D core memory as found in the IBM-4 AP-101 basic configuration is shown in Figure 5.5-1. This partitioning divides the memory into the timing page and four storage pages.

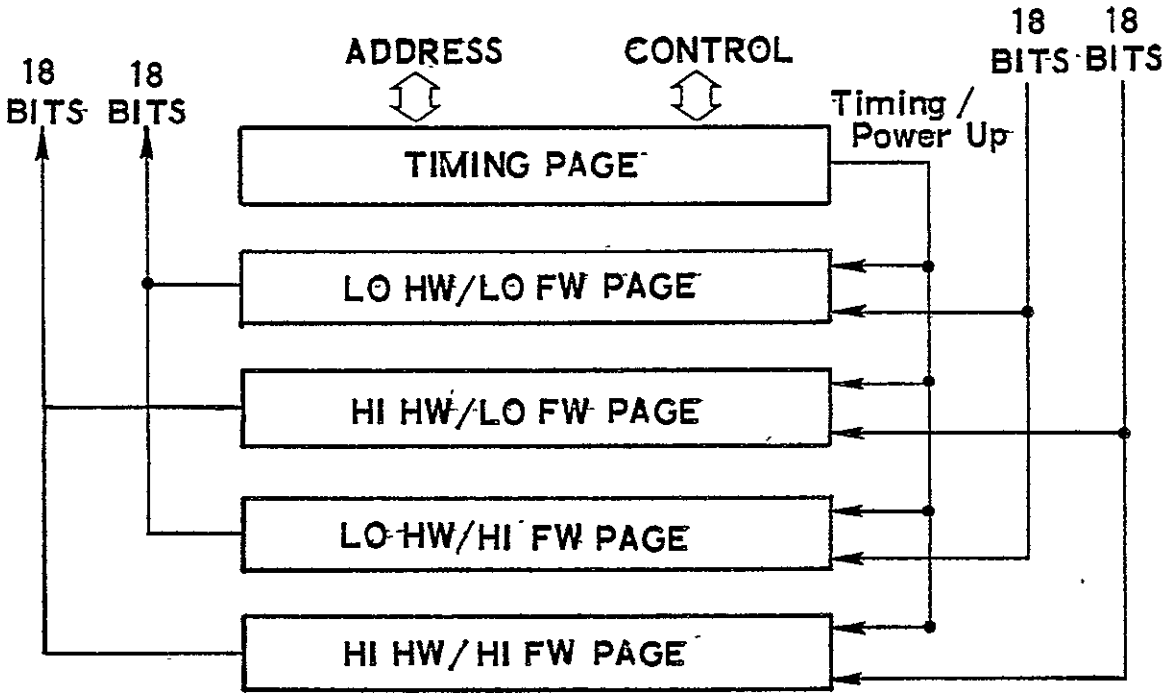


FIGURE 5.5-1 PARTITIONING THE AP-101 MEMORY

Further partitioning continues as shown in Figure 5.5-2 for a storage page. We see from this partitioning that a transient in the output buffer will only corrupt the memory output, but a transient in the data register would surely corrupt memory during the restore cycle as well as the memory output.

Consider the case of a Y-driver as shown in Figure 5.5-3. If a transient strikes a powered Y-driver, then any Y-driver failure mode will corrupt memory during the read and/or restore cycle. The quantity β_{ij} for a Y-driver then becomes the probability that it is selected while a transient is active. The Y-driver on the page has a 1/32 probability of being used, and for a 16K memory, the page of the driver of interest has a 50 percent probability of being used. If we assume program words are accessed every 3 μs, then the quantity β_{ij} for one Y-driver becomes

$$\beta_{ij} = 1 = \sum_{n=1}^{\infty} \left(\frac{63}{64}\right)^n P(Td=3n\ \mu s)$$

where Td is a discrete random variable representing transient duration. If we assume it is uniform from 3 μs to 300 μs at intervals of 3 μs for ease of computation, then β_{ij} becomes

$$\beta_{ij} = 1 - \frac{1}{100}\sum_{n=1}^{100} \left(\frac{63}{64}\right)^n = .57$$

Computing the β's as above for the remaining functional components and finding the β_{ij}'s as is done for permanent faults, program integrity is found to be .30.

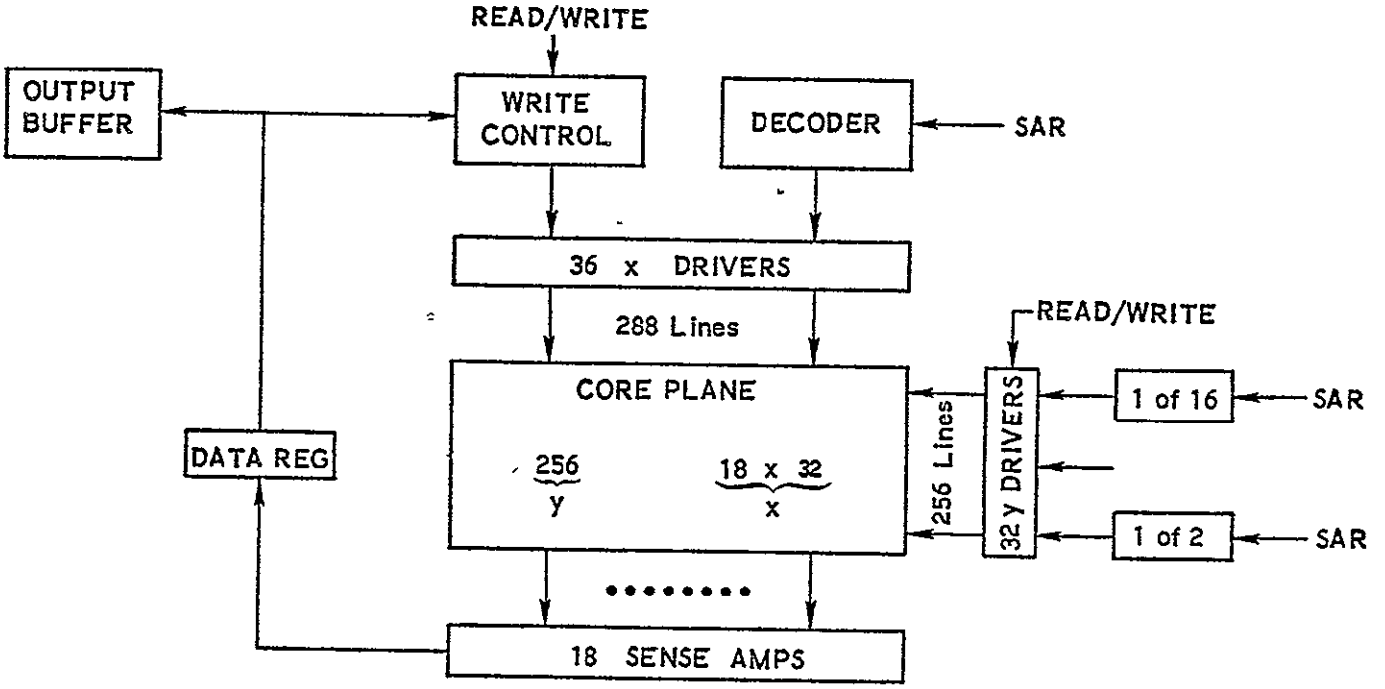


FIGURE 5.5-2 . PARTITIONING OF THE AP-101 MEMORY STORAGE-PAGE

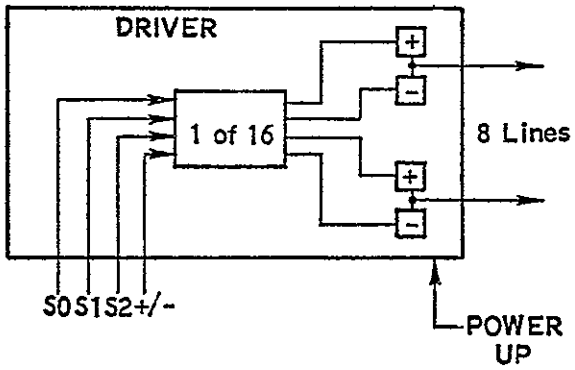


FIGURE 5.5-3 Y-DRIVER ANALYSIS

5.5.3 INTERPRETATION OF SIMULATOR OUTPUT

The simulation results are only meaningful when examined with the system configuration defined by the input deck. Thus, of the six pages of simulator output, four pages are devoted to describing the configurations of the software, GPCs, and flight critical devices. Figure 5.5-4 on the facing page shows a simulator produced summary of the GPC configuration for the baseline simulator run.

The top line (in this case "QUADRUPLEX") indicates the basic configuration of the GPCs. In this case, "QUADRUPLEX" indicates that there are four GPCs, all of which perform identical operations and compare the results for fault detection and isolation. "TRIPLEX WITH 2 SPARES" would indicate that the redundant set consisted of three computers; but in addition, two spares are included that are either powered down or perform non-critical computations until a failure occurs in one of the redundant computers. A spare is then chosen to replace the faulty computer. The "TRIPLEX WITH 2 SPARES" configuration could be used for non-critical mission phases. The next two lines indicate that 500,000 6-hour missions were simulated.

The next section of output is headed by "TRANSIENT RECOVERY PROCEDURES." It lists the transient recovery procedures in use and their performance characteristics. The baseline system uses two transient recovery methods. "DELAY RECONFIGURATION" indicates that reconfiguration doesn't occur unless two faults within a specified time interval. Thus, transients causing data errors which are compensated by the control loop calculations after an iteration will not cause the loss of a computer. The DURATION indicates a 1.0 millisecond overhead to do this recovery procedure. The RECURRENCE INTERVAL indicates that if two faults occur in the same computer within a 1280 millisecond period, the second fault is assumed to be a recurrence of the first fault and will cause system degradation. An EFFECTIVENESS of 0.5 indicates that half of the transient faults that do not cause damage to the program can be "corrected" (i.e., not cause unnecessary system degradation) by this procedure. A SYSTEM RESTART which is invoked because of multiple faults where the faulty computer cannot be isolated. One thousand milliseconds is required for a SYSTEM RESTART. MEMORY-COPY, ROLLAHEAD, AND ROLLBACK can also be incorporated into the system configuration as transient recovery procedures. If they are, they will be listed in this section along with their characteristics.

QUADRUPLEX

```
NUMBER OF MISSIONS          500000
MISSION DURATION          6.0000 HOURS


TRANSIENT RECOVERY PROCEDURES

    DELAY RECONFIGURATION
       DURATION                      1.00 MILLISECONDS
       RECURRENCE INTERVAL        1280.00 MILLISECONDS
       EFFECTIVENESS              .500000

    SYSTEM RESTART
       DURATION                   1000.00 MILLISECONDS


RECOVERY  PARAMETERS

    PROGRAM SURVIVABILITY         .100000

    PROBABILITY OF FAULT DETECTION BY BITE
       CENTRAL PROCESSOR           .458
       MEMORY                      .981
       I/O PROCESSOR             -0.000

    STP EFFICIENCY                .919000
    MEAN DIAGNOSIS TIME              6.50 MILLISECONDS
    DELAY BEFORE RECOVERY            0.00 MILLISECONDS
    ISOLATION DURATION               0.00 MILLISECONDS

SOFTWARE PARAMETERS
    ITERATION PERIOD                40.00 MILLISECONDS
    MINOR CYCLE DURATION            40.00 MILLISECONDS
    MAJOR CYCLE DURATION               32 ITERATIONS
    TIME BETWEEN COMPARISONS        40.00 MILLISECONDS
    MAXIMUM DOWN TIME             1000.00 MILLISECONDS
    MINOR CYCLE PROGRAM SIZE      .500000
    ASYNCHRONOUS EXECUTIVE - INTERRUPT RATE   100.0 PER SECOND

DEDICATED I/O PROCESSORS
```

FIGURE 5.5-4 CONFIGURATION SUMMARY - PART 1

"RECOVERY PARAMETERS" heads the next section of the GPC configuration summary. Here the program survivability, the BITE fault detection probabilities and the Self Test Program (STP) characteristics are listed. The PROGRAM SURVIVABILITY represents the probability that the program survives given that a memory transient occurs. Since the main memory is CORE DRO, every word read from memory must be re-written into memory by the hardware. Thus, if an error occurs during the read cycle of an instruction, it is written back into memory corrupting the program. This is reflected by a low value of program survivability (0.1). According to the listing, BITE has a probability of 0.458 for detecting CPU faults and a probability of 0.981 for detecting memory faults. Negative zero indicates that the parameters was unspecified. The STP EFFICIENCY indicates that the probability of detecting a fault by means of a computer self test (software) is 0.919. If a computer is faulty, this fact will be detected in an average duration of 6.5 milliseconds. The ISOLATION DURATION of zero indicates that once a fault is detected, its isolation of nearly immediate. DELAY BEFORE RECOVERY indicates the amount of time transient recovery is delayed in order to allow the transient to become inactive. In this case there is no delay.

Under "SOFTWARE PARAMETERS" are listed the assumed values for the ITERATION PERIOD, the MINOR CYCLE DURATION, the MAJOR CYCLE DURATION, the TIME BETWEEN COMPARISONS, the MAXIMUM DOWN TIME, the relative MINOR CYCLE PROGRAM SIZE, the the type of executive structures. The ITERATION PERIOD, which specifies the time between consecutive major control loop calculations, is assumed to be the same as the MINOR CYCLE DURATION, which is 40 milliseconds. The major cycle consists of 32 minor cycles and thus lasts 1280 milliseconds. It was assumed that there is one comparison every minor cycle; thus the TIME BETWEEN COMPARISONS is 40.00 milliseconds. The MINOR CYCLE PROGRAM SIZE indicates that half of the computer time is spent executing minor cycle calculations. The software structure is ASYNCHRONOUS with an average rate of a hundred interrupts per second. The system must recover in less than a second in order to avoid system failure. This is specified by the MAXIMUM DOWN TIME being 1000 milliseconds. DEDICATED I/O PROCESSORS indicate that an input-output processor is dedicated to each of the computers.

QUADRUPLEX

NUMBER OF MISSIONS 500000
MISSION DURATION 6.0000 HOURS

TRANSIENT RECOVERY PROCEDURES

DELAY RECONFIGURATION
DURATION 1.00 MILLISECONDS
RECURRENCE INTERVAL 1280.00 MILLISECONDS
EFFECTIVENESS .500000

SYSTEM RESTART
DURATION 1000.00 MILLISECONDS

RECOVERY PARAMETERS

PROGRAM SURVIVABILITY .100000

PROBABILITY OF FAULT DETECTION BY BITE
CENTRAL PROCESSOR .458
MEMORY .991
I/O PROCESSOR -0.000

STP EFFICIENCY .919000
MEAN DIAGNOSIS TIME 6.50 MILLISECONDS
DELAY BEFORE RECOVERY 0.00 MILLISECONDS
ISOLATION DURATION 0.00 MILLISECONDS

SOFTWARE PARAMETERS
ITERATION PERIOD 40.00 MILLISECONDS
MINOR CYCLE DURATION 40.00 MILLISECONDS
MAJOR CYCLE DURATION 32 ITERATIONS
TIME BETWEEN COMPARISONS 40.00 MILLISECONDS
MAXIMUM DOWN TIME 1000.00 MILLISECONDS
MINOR CYCLE PROGRAM SIZE .500000
ASYNCHRONOUS EXECUTIVE - INTERRUPT RATE 100.0 PER SECOND

DEDICATED I/O PROCESSORS

FIGURE 5.5-4 CONFIGURATION SUMMARY - PART 1

Figure 5.5-5 lists the failure rates for each of the GPC devices. NOTATIONS defines what is meant by MODULE 1, MODULE 2 and MODULE 3. The impact of I/O processor faults represents the probability that an IOP fault affects the computer, a bus, or both the computer and a bus. Here it was assumed that all IOP faults affect the computer but not the bus. The DESCRIPTION OF THE FAULTY ENVIRONMENT lists the permanent failure rate, the transients failure rate and the average transient duration for each of the CPU, the IOP, and the memory.

The failure rates of the devices for the flight critical bus partition are listed in Figure 5.5-6 which is Page 3 of the simulator output. The NET PERMANENT FAILURE RATE represents the total failure rate of all of the devices taking into account their redundancy. Thus, the ADTAs failure rate is included four times in the net failure rate calculation because there are four ADTA. All failure rates are listed in number of failures per million hours. The ADTA (Air Data Transducer) has a permanent failure rate of 250 failures per million hours. The MDMs and DDUs each have two permanent failure rates associated with them. The first number indicates the failure rate of the main body of the MDM and the second number indicates the failure rate of the redundant portion of the MDM associated with each FC bus interface. For the baseline run, all flight critical device transient failure rates were assumed to be zero. This was done because nearly all transient faults will not cause system degradation. The -0.00 in each column indicates that the input was not specified.

```
NOTATIONS
    MODULE 1 - CENTRAL PROCESSING UNIT
    MODULE 2 - I/O PROCESSOR
    MODULE 3 - MEMORY
    MODULE 4 - EXTERNAL DEVICES

IMPACT OF I/O PROCESSOR FAULTS
    ON COMPUTER              1.000000
    ON BUS                   0.000000
    ON BUS AND COMPUTER      0.000000


DESCRIPTION OF THE FAULT ENVIRONMENT
    MODULE  1 : PERMANENT RATE          .12E-03 PER HOUR
                TRANSIENT RATE          .12E-03 PER HOUR
                TRANSIENT DURATION      .10E+00 MILLISECONDS (EXPONENTIAL)
    MODULE  2 : PERMANENT RATE          .44E-03 PER HOUR
                TRANSIENT RATE          .44E-03 PER HOUR
                TRANSIENT DURATION      .10E+00 MILLISECONDS (EXPONENTIAL)
    MODULE  3 : PERMANENT RATE          .44E-03 PER HOUR
                TRANSIENT RATE          .44E-03 PER HOUR
                TRANSIENT DURATION      .10E+00 MILLISECONDS (EXPONENTIAL)
```

FIGURE 5.5-5 CONFIGURATION SUMMARY - PART 2

FLIGHT CRITICAL BUS PARTITION --- FAILURE RATES

NET PERMANENT FAILURE RATE 9998.95 PER MILLION HRS

NET TRANSIENT FAILURE RATE 0.00 PER MILLION HRS

DEVICE	PERMANENT RATE		TRANSIENT RATE	
FC-BUS 1	.10		-0.00	
FC-BUS 2	.10		-0.00	
FC-BUS 3	.10		-0.00	
FC-BUS 4	.10		-0.00	
FC-BUS 5	.10		-0.00	
FC-BUS 6	.10		-0.00	
FC-BUS 7	.10		-0.00	
FC-BUS 8	.10		-0.00	
ADU 1	55.60	5.00	-0.00	-0.00
ADU 2	55.60	5.00	-0.00	-0.00
MDM FC-1	155.95	74.16	-0.00	-0.00
MDM FC-2	155.95	74.16	-0.00	-0.00
MDM FC-3	155.95	74.16	-0.00	-0.00
MDM FC-4	87.25	74.16	-0.00	-0.00
MDM FA-1	144.42	74.16	-0.00	-0.00
MDM FA-2	144.42	74.16	-0.00	-0.00
MDM FA-3	144.42	74.16	-0.00	-0.00
MDM FA-4	125.57	74.16	-0.00	-0.00
AVVI	75.70		-0.00	
AMI	93.20		-0.00	
HSI	40.00		-0.00	
ADI	56.50		-0.00	
APTA	250.00		-0.00	
ACCEL	109.50		-0.00	
IMU	285.70		-0.00	
TACAN	1000.00		-0.00	
MSPLS	500.00		-0.00	
	0.00		-0.00	
MTU	0.00	0.00	-0.00	-0.00
RHC	.10	2.00	-0.00	-0.00
RPTA	.10	2.00	-0.00	-0.00
SRTC	.10	2.00	-0.00	-0.00
ASA	100.00		-0.00	
RGYRO	66.70		-0.00	

FIGURE 5.5-6 CONFIGURATION SUMMARY - PART 3

Figure 5.5-7 illustrates the fourth page of simulator output. It lists the assumed transient leakages, permanent coverages, and fault detection probabilities for each of the devices in the flight critical bus partition. Two leakages and coverages are specified for the MDMs and DDUs. The first column represents the leakage/coverage for a fault occurring in the non-redundant portion of the BTU. The second column represents the leakage/coverage for a fault cocurring in the redundant portion of the BTU. The DDU devices (i.e., AVVI, AMI, HSI and ADI) have two transient detection probabilities associated with them: the first number of the transient detectability when two devices are active. Similarly, the dedicated devices on the flight forward MDMs have four transient detectabilities associated with the probability of detecting a fault in when one, two three or four devices are active respectively. There are three permanent coverages for each device: the first is the probability of recovery from a permanent fault when two devices are active; the second is the coverage when three devices are active; and the third is the coverage when four devices are active.

COVERAGE PARAMETERS --- FLIGHT CRITICAL BUS PARTITION

BUS TRANSIENT LEAKAGE 0.000000

BUS PERMANENT COVERAGE .999000

BTU NAME	TRANSIENT LEAKAGE		PERMANENT COVERAGE	
DDU 1	0.000000	0.000000	.999000	.999000
DDU 2	0.000000	0.000000	.999000	.999000
MDM FF-1	0.000000	0.000000	.999000	.999000
MDM FF-2	0.000000	0.000000	.999000	.999000
MDM FF-3	0.000000	0.000000	.999000	.999000
MDM FF-4	0.000000	0.000000	.999000	.999000
MDM FA-1	0.000000	0.000000	.999000	.999000
MDM FA-2	0.000000	0.000000	.999000	.999000
MDM FA-3	0.000000	0.000000	.999000	.999000
MDM FA-4	0.000000	0.000000	.999000	.999000

DDU DEVICE	TRANSIENT DETECTION	TRANSIENT LEAKAGE	PERMANENT COVERAGE
AVVI	.950000	.999000	0.000000	.999000
AMI	.950000	.999000	0.000000	.999000
HSI	.950000	.999000	0.000000	.999000
ADI	.950000	.999000	0.000000	.999000

DEVICE	TRANSIENT DETECTION				TRANSIENT LEAKAGE	PERMANENT COVERAGE		
ADTA	.950000	.999000	.999000	.999000	0.000000	.950000	.999000	.999000
ACCEL	.950000	.999000	.999000	.999000	0.000000	.950000	.999000	.999000
IMU	.950000	.999000	.999000	.999000	0.000000	.950000	.999000	.999000
TACAN	.950000	.999000	.999000	.999000	0.000000	.950000	.999000	.999000
MSBLS	.950000	.999000	.999000	.999000	0.000000	.950000	.999000	.999000
	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000

DEVICE	TRANSIENT DETECTION		TRANSIENT LEAKAGE		PERMANENT DETECTION	PERMANENT COVERAGE
MTU	.999000	.999000	0.000000	0.000000	.999000	.999000
RHC	.999000	.999000	0.000000	0.000000	.999000	.999000
RPTA	.999000	.999000	0.000000	0.000000	.999000	.999000
SBTC	.999000	.999000	0.000000	0.000000	.999000	.999000

DEVICE	TRANSIENT DETECTION	TRANSIENT LEAKAGE	PERMANENT COVERAGE
ASA	.999000	0.000000	.950000
RGYRO	.999000	0.000000	.950000

FIGURE 5.5-7 CONFIGURATION SUMMARY - PART 4

Figure 5.5-8 shows the first page of output statistics that was generated by the simulator. The top four lines indicate the number of faults that occur in the entire system including both the GPC partition and the FCB partition. In this case, a total of 53,595 faults occurred during the simulation of 500,000 missions. Only 35 system failures occurred as a result of all of these faults.

The next section which is headed by "GPC FAULT AND RECOVERY STATISTICS" lists several statistics for each state of the configuration (i.e., for quadruplex, residue triplex, residue duplex, and residue simplex). The columns headed "PERMANENT FAULTS," "TRANSIENT FAULTS," and "TOTAL FAULTS" list the number of faults that occur for each of the GPC configurations. The "SYSTEM FAILURES" column lists the number of flight-critical failures that occurred for each GPC configuration. The number of transients resulting in system degradation are listed in the column entitled "LEAKY TRANSIENTS." The "DEGRADATIONS TO" column lists the number of times the configuration degraded to each GPC redundancy level as because of a fault. Thus, while the GPCs were in the initial configuration (quadruplex), they sustained 11,546 permanent GPC faults and 11,752 transient faults. Of the 11,752 transient faults, 8,179 of them resulted in system degradation. Thus there were 8,179 + 11,546 = 19,725 system degradations from quadruplex. By examining the "DEGRADATIONS TO" column, it can be seen that all degradations from quadruplex were to triplex. For this calculation, it was assumed that all 8,179 leaky transients and 11,546 permanents resulted in system degradation. The GPC recovery procedure statistics list the number of times each of the transient recovery procedures was invoked.

The estimated mission failure probability, transient leakages, and coverages all have a confidence interval associated with them. The mission success probability is calculated by finding the ratio of the number of system failures to the total number of missions. The simulation statistics indicate that the mission failure probability is 0.000072 ± 0.000024. This indicates that the system failure probability falls between 4.8×10^{-5} and 9.6×10^{-5} with a 95% confidence. This is not the exact confidence interval, but a close estimate that assumes a large number of tries (see [FREU 62] for details).

S I M U L A T I O N S T A T I S T I C S

NUMBER OF PERMANENTS 41567
NUMBER OF TRANSIENTS 11928
TOTAL NUMBER OF FAULTS 53595
NUMBER OF SYSTEM FAILURES 34

GPC FAULT AND RECOVERY STATISTICS

CONFIGURATION	PERMANENT FAULTS	TRANSIENT FAULTS	TOTAL FAULTS
QUADRUPLEX	11546	11752	23298
TRIPLEX	184	174	358
DUPLEX	0	2	2
SIMPLEX	0	0	0

	SYSTEM FAILURES	LEAKY TRANSIENTS	DEGRADATIONS TO
QUADRUPLEX	0	8179	0
TRIPLEX	0	123	19725
DUPLEX	0	2	307
SIMPLEX	0	0	2

GPC RECOVERY PROCEDURE STATISTICS
NUMBER OF DELAY-RECOVERYS 23712
NUMBER OF SYSTEM RESTARTS 0

PROPORTION OF MISSED ITERATIONS .107E-08
LONGEST SERIES OF MISSED ITERATIONS 1

MISSION FAILURE PROBABILITY .00207200 +/- .00002366

LEAKAGES
MULTIPLEX .69606335 +/- .03842197
DUPLEX .66666667 +/- .33333333
SIMPLEX *.00000000 +/- *.00000000

COVERAGES
MULTIPLEX .99990018 +/- .00009982
DUPLEX .66666667 +/- .33333333

FIGURE 5.5-8 SIMULATOR STATISTICS

Figure 5.5-9 shows the mission statistics generated for the FCB partition. The number of flight-critical failures indicates that 35 system failures occurred because of faults in the FCB partition. Of these, six occurred because of uncovered faults (i.e., faults that were not detected), and twenty-eight occurred because of faults that were detected, but not covered. The latter number was obtained by adding the number in the "UNCOVERED PERMANENTS" column. For each device, the number of transients, permanents, leaky transients, and uncovered permanents are listed. Here, the number of transients and leaky transients for each device is zero, because the transient failure rate was assumed to be zero. The number of permanent faults and system failures occurring in a specific device type are listed in the appropriate row. Thus, 9,027 faults occurred in the TACANs, and there were 13 system failures because of inadequate TACAN coverage or TACAN redundancy.

FLIGHT CRITICAL BUS PARTITION --- MISSION STATISTICS

TRANSIENT FAULTS 11928
PERMANENT FAULTS 41667
TOTAL FAULTS 53595

NUMBER OF FLIGHT CRITICAL FAILURES 34

UNCOVERED SYSTEM FAILURES 6

BUS	0
BTU	5
DDU DEVICE	1
FF-MDM DEVICE	
DEDICATED	0
NON-DEDICATED	0
FA-MDM DEVICE	0

	TRANSIENT	PERMANENT	UNCOVERED TRANSIENT	UNCOVERED PERMANENT
BUS	0	4	0	0
DDU	0	419	0	0
AVVI	0	405	0	0
AMI	0	543	0	1
HSI	0	249	0	0
ADI	0	328	0	1
FF-MDM	0	3472	0	0
ADTA	0	2955	0	4
ACCEL	0	1026	0	1
IMU	0	2547	0	4
TACAN	0	9027	0	13
MSBLS	0	4489	0	4
	0	0	0	0
MTU	0	0	0	0
RHC	0	35	0	0
RPTA	0	40	0	0
SBTC	0	37	0	0
FA-MDM	0	2596	0	0
ASA	0	1142	0	0
RGYRO	0	623	0	0

NUMBER OF FAULTS/MISSION	1	2	3	4	5	6	7	8	9	10
NUMBER OF MISSIONS	28241	845	18	1	0	0	0	0	0	0
NUMBER OF SYSTEM FAILURES	23	10	1	0	0	0	0	0	0	0

FIGURE 5.5-9 FLIGHT CRITICAL BUS STATISTICS

6.0 DPS SURVIVABILITY ESTIMATES

6.1 BASELINE PARAMETER APPROACH

In order to make mission success probability calculations using the analytic models described in Section 4 and the simulation models described in Section 5, it is necessary to obtain values for the various parameters required in these models. The approach taken was to obtain a baseline set of parameters and then vary these parameters to reflect the several options investigated. Because the Shuttle ALT configuration has been approved through the various design reviews and is in the process of being brought into being, this configuration was chosen as the baseline from which variations would be made.

The parameter values used for the baseline configuration were obtained using four different approaches. These are: (1) contractor's direct estimate; (2) NASA estimate; (3) Ultrasystems direct estimate; and (4) Ultrasystems estimate. One might wonder why approach 1, contractor's direct estimate, was not used for all parameter determinations. It was not used beacuse MTTF, or its reciprocal, the failure rate, was not required for each unit. However, there were contractors who had supplied this information and thus where available, it was used. The adjective "direct" is used to indicate that the estimate was obtained by a detailed analysis, e.g., use of individual part failure rates when estimating an overall unit failure rate. Estimates not labelled "direct" were obtained by comparison of comparable equipment. All contractor direct estimates and NASA estimates were obtained from the Project Monitor for this contract. Ultrasystems direct estimates were made for corroborative purposes for selected units. Ultrasystems estimates (non-direct) were made where other estimates were not obtainable.

The two primary categories of parameters for which estimates were obtained were unit permanent failure rates, and unit self-test program effectiveness. Where unit permanent failure rates were not available from either contractor direct estimates or NASA estimates, Ultrasystems estimated the values using the assumption that equipments that were mechanized using similar technologies would have failure rates that are proportional to weight. It is thought that this is a reasonable assumption. All estimates of unit self-test program effectiveness were from contractor direct estimates.

A computer listing of the baseline parameters is shown in Figure 6.1-1.

CONFIGURATION PARTICULARS

UNIT NAME	PERMANENT RATE	TRANSIENT RATE
MCDSDU	.2210000E-03	0.
MCDSKR	.1786000E-05	0.
GPC	.9910000E-03	.9910000E-03
FF MDM	.2300000E-03	0.
ADTA	.2500000E-03	0.
ACCEL	.1100000E-03	0.
IMU	.2950000E-03	0.
TACAN	.1000000E-02	0.
MSBLS	.5000000E-03	0.
RHC	.2000000E-05	0.
RPTA	.2300000E-05	0.
SBTC	.2000000E-05	0.
FA MDM	.2200000E-03	0.
ASA	.1000000E-03	0.
RGYRO	.6670000E-04	0.
DDU	.5560000E-04	0.
AVVI	.7570000E-04	0.
A/MI	.9320000E-04	0.
HSI	.4080000E-04	0.
ADI	.5650000E-04	0.
PCMMU	.8620000E-03	0.
OF MDM	.1500000E-03	0.
OA MDM	.1500000E-03	0.

FIGURE 6.1-1

BASELINE PARAMETER VALUES

	SUBSCRIPT	DETECTABILITY	DIAGNOSABILITY	RECOVERABILITY	LEAKAGE
MCDSDU	2	.9990000	.9770000	1.0000000	0.0000000
MCDSDU	3	.9990000	1.0000000	1.0000000	0.0000000
MCDSKR	2	1.0000000	1.0000000	1.0000000	0.0000000
GPC	2	1.0000000	.9140000	1.0000000	.7030000
GPC	3	1.0000000	1.0000000	1.0000000	.7030000
GPC	4	1.0000000	1.0000000	1.0000000	.7030000
FF MDM	2	.9990000	.9500000	1.0000000	0.0000000
FF MDM	3	.9990000	1.0000000	1.0000000	0.0000000
FF MDM	4	.9990000	1.0000000	1.0000000	0.0000000
ADTA	2	.9990000	.9500000	1.0000000	0.0000000
ADTA	3	.9990000	1.0000000	1.0000000	0.0000000
ADTA	4	.9990000	1.0000000	1.0000000	0.0000000
ACCEL	2	.9990000	.9500000	1.0000000	0.0000000
ACCEL	3	.9990000	1.0000000	1.0000000	0.0000000
IMU	2	.9990000	.9500000	1.0000000	0.0000000
IMU	3	.9990000	1.0000000	1.0000000	0.0000000
TACAN	2	.9990000	.9500000	1.0000000	0.0000000
TACAN	3	.9990000	1.0000000	1.0000000	0.0000000
MSBLS	2	.9990000	.9500000	1.0000000	0.0000000
MSBLS	3	.9990000	1.0000000	1.0000000	0.0000000
RHC	2	.9990000	.9500000	1.0000000	0.0000000
RHC	3	.9990000	1.0000000	1.0000000	0.0000000
RPTA	2	.9990000	.9500000	1.0000000	0.0000000
RPTA	3	.9990000	1.0000000	1.0000000	0.0000000
SBTC	2	.9990000	.9500000	1.0000000	0.0000000
SBTC	3	.9990000	1.0000000	1.0000000	0.0000000
FA MDM	2	.9990000	.9500000	1.0000000	0.0000000
FA MDM	3	.9990000	1.0000000	1.0000000	0.0000000
FA MDM	4	.9990000	1.0000000	1.0000000	0.0000000
ASA	2	.9990000	.9500000	1.0000000	0.0000000
ASA	3	.9990000	1.0000000	1.0000000	0.0000000
ASA	4	.9990000	1.0000000	1.0000000	0.0000000
RGYRO	2	.9990000	.9500000	1.0000000	0.0000000
RGYRO	3	.9990000	1.0000000	1.0000000	0.0000000
DDU	2	.9990000	.9990000	1.0000000	0.0000000
AVVI	2	.9990000	.9990000	1.0000000	0.0000000
A/MI	2	.9990000	.9990000	1.0000000	0.0000000
HSI	2	.9990000	.9990000	1.0000000	0.0000000
ADI	2	.9990000	.9990000	1.0000000	0.0000000
PCMMU	2	.9990000	.9990000	1.0000000	0.0000000
OF MDM	2	.9990000	.9990000	1.0000000	0.0000000
OA MDM	2	.9990000	.9990000	1.0000000	0.0000000

6.2 BASELINE RESULTS

The flight-critical-bus simulation and analytic model are cross-checked using the baseline parameter set as a basis on which to verify their accuracy. Agreement between these two approaches means that the modeling approach discussed in Section 4.4 is a valid approximation. For the baseline parameter set, the forward flight-critical-bus analytic model predicts a survivability of .9999423 while the simulator yields a result of .9999437. Thus they differ by only 14 parts in 10^7. These results certainly agree within the accuracy of the Monte Carlo simulation.

The survivability results for the baseline configuration are given in the listings that follow. In these listings, survivability and failure probability versus mission times from one to twenty hours is given for each partition and flight critical device. (Failure probability is the converse of survivability, i.e. FP(T) = 1 - S(T).) There are twenty-seven printout pages in all.

There are several interesting features of these results that are summarized on the opposite page. The GPC set, with a detectability of 1, has a failure probability two orders of magnitude better than the TACAN set, with a detectability of .999, the design goal. The GPC and TACAN have similar failure rates. Variations of detectability will be studied in a later section.

The TACAN and MSBLS, with relatively high failure rates, account for 57% of the forward flight critical failure probability. The hand controls add only a miniscule amount to the total failure probability. The forward flight critical MDM system contributes 71.6% of the total safety-critical failure probability, a very significant amount that is primarily due to the large TACAN and MSBLS failure rates.

The aft flight critical MDM system partition, the flight displays, and the MCDS contribute a much smaller percentage to the overall safety critical failure probability, i.e. 11.1%, 11.8%, and 5.1%, respectively. The GPC contribution is a miniscule .4%.

Mission critical functions are not as important in ALT as they are in orbital flights. About the only loss sustained would be some telemetry data.

SUMMARY OF SHUTTLE (ALT) AVIONICS SURVIVABILITIES
FOR A SIX-HOUR MISSION

Unit	Failure Probability	Percent of Total Safety Critical
GPC	$3.5(10)^{-7}$	.4
TACAN	$2.3(10)^{-5}$	N/A
MSBLS	$1.0(10)^{-5}$	N/A
FWD FLIGHT CRITICAL	$5.80(10)^{-5}$	71.6
AFT FLIGHT CRITICAL	$9.0(10)^{-6}$	11.1
FLIGHT DISPLAYS	$9.58(10)^{-6}$	11.8
MCDS	$4.1(10)^{-6}$	5.1
SAFETY CRITICAL	$8.10(10)^{-5}$	100.0
MISSION CRITICAL	$1.4(10)^{-4}$	N/A

SURVIVABILITY FOR MODS

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.666320E-06
2.000000	.999999	.133332E-05
3.000000	.999998	.201995E-05
4.000000	.999997	.273557E-05
5.000000	.999997	.339895E-05
6.000000	.999996	.409922E-05
7.000000	.999995	.480646E-05
8.000000	.999994	.552971E-05
9.000000	.999994	.624203E-05
10.000000	.999993	.697048E-05
11.000000	.999992	.770611E-05
12.000000	.999992	.844890E-05
13.000000	.999991	.919916E-05
14.000000	.999990	.995668E-05
15.000000	.999989	.107216E-04
16.000000	.999989	.114940E-04
17.000000	.999988	.122739E-04
18.000000	.999987	.130614E-04
19.000000	.999986	.138565E-04
20.000000	.999985	.146593E-04

SURVIVABILITY FOR GPC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.165165E-08
2.000000	1.000000	.131978E-07
3.000000	1.000000	.444936E-07
4.000000	1.000000	.105336E-06
5.000000	1.000000	.205493E-06
6.000000	1.000000	.354674E-06
7.000000	.999999	.562545E-06
8.000000	.999999	.838726E-06
9.000000	.999999	.119279E-05
10.000000	.999998	.163426E-05
11.000000	.999998	.217261E-05
12.000000	.999997	.281728E-05
13.000000	.999996	.357764E-05
14.000000	.999996	.446304E-05
15.000000	.999995	.548277E-05
16.000000	.999993	.664605E-05
17.000000	.999992	.796219E-05
18.000000	.999991	.944007E-05
19.000000	.999989	.110896E-04
20.000000	.999987	.129180E-04

SURVIVABILITY FOR FF MOM

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.919895E-06
2.000000	.999998	.183960E-05
3.000000	.999997	.275911E-05
4.000000	.999996	.367846E-05
5.000000	.999995	.459765E-05
6.000000	.999994	.551671E-05
7.000000	.999994	.643564E-05
8.000000	.999993	.735446E-05
9.000000	.999992	.827319E-05
10.000000	.999991	.919184E-05
11.000000	.999990	.101104E-04
12.000000	.999989	.110290E-04
13.000000	.999988	.119475E-04
14.000000	.999987	.128659E-04
15.000000	.999986	.137844E-04
16.000000	.999985	.147029E-04
17.000000	.999984	.156214E-04
18.000000	.999983	.165400E-04
19.000000	.999983	.174586E-04
20.000000	.999982	.183772E-04

SURVIVABILITY FOR ADTA

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.999878E-06
2.000000	.999998	.199952E-05
3.000000	.999997	.299896E-05
4.000000	.999996	.399819E-05
5.000000	.999995	.499726E-05
6.000000	.999994	.599616E-05
7.000000	.999993	.699493E-05
8.000000	.999992	.799358E-05
9.000000	.999991	.899214E-05
10.000000	.999990	.999061E-05
11.000000	.999989	.109890E-04
12.000000	.999988	.119874E-04
13.000000	.999987	.129857E-04
14.000000	.999986	.139841E-04
15.000000	.999985	.149824E-04
16.000000	.999984	.159808E-04
17.000000	.999983	.169793E-04
18.000000	.999982	.179778E-04
19.000000	.999981	.189764E-04
20.000000	.999980	.199752E-04

SURVIVABILITY FOR ACCEL

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.331794E-06
2.000000	.999999	.667189E-06
3.000000	.999999	.100616E-05
4.000000	.999999	.134875E-05
5.000000	.999998	.169495E-05
6.000000	.999998	.204476E-05
7.000000	.999998	.239818E-05
8.000000	.999997	.275524E-05
9.000000	.999997	.311592E-05
10.000000	.999997	.348025E-05
11.000000	.999996	.384821E-05
12.000000	.999996	.421982E-05
13.000000	.999995	.459508E-05
14.000000	.999995	.497401E-05
15.000000	.999995	.535659E-05
16.000000	.999994	.574285E-05
17.000000	.999994	.613278E-05
18.000000	.999993	.652639E-05
19.000000	.999993	.692369E-05
20.000000	.999993	.732468E-05

SURVIVABILITY FOR IMU

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.870138E-06
2.000000	.999998	.176462E-05
3.000000	.999997	.268354E-05
4.000000	.999996	.362699E-05
5.000000	.999995	.459508E-05
6.000000	.999994	.558791E-05
7.000000	.999993	.660556E-05
8.000000	.999992	.764813E-05
9.000000	.999991	.871573E-05
10.000000	.999990	.980845E-05
11.000000	.999989	.109264E-04
12.000000	.999988	.120696E-04
13.000000	.999987	.132383E-04
14.000000	.999986	.144324E-04
15.000000	.999984	.156522E-04
16.000000	.999983	.168976E-04
17.000000	.999982	.181688E-04
18.000000	.999981	.194659E-04
19.000000	.999979	.207890E-04
20.000000	.999978	.221382E-04

SURVIVABILITY FOR TACAN

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999997	.314889E-05
2.000000	.999993	.659835E-05
3.000000	.999990	.103525E-04
4.000000	.999986	.144155E-04
5.000000	.999981	.187915E-04
6.000000	.999977	.234844E-04
7.000000	.999972	.284983E-04
8.000000	.999966	.333372E-04
9.000000	.999960	.395052E-04
10.000000	.999954	.455061E-04
11.000000	.999948	.519439E-04
12.000000	.999941	.585224E-04
13.000000	.999934	.655456E-04
14.000000	.999927	.729173E-04
15.000000	.999919	.806413E-04
16.000000	.999911	.887214E-04
17.000000	.999903	.971613E-04
18.000000	.999894	.105965E-03
19.000000	.999885	.115136E-03
20.000000	.999875	.124678E-03

SURVIVABILITY FOR MSBLS

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999998	.153714E-05
2.000000	.999997	.314889E-05
3.000000	.999995	.483579E-05
4.000000	.999993	.658835E-05
5.000000	.999992	.843739E-05
6.000000	.999990	.103525E-04
7.000000	.999988	.123452E-04
8.000000	.999986	.144155E-04
9.000000	.999983	.165641E-04
10.000000	.999981	.187915E-04
11.000000	.999979	.210988E-04
12.000000	.999977	.234844E-04
13.000000	.999974	.259519F-04
14.000000	.999972	.284983E-04
15.000000	.999969	.311269F-04
16.000000	.999966	.338372E-04
17.000000	.999963	.366238E-04
18.000000	.999960	.395052E-04
19.000000	.999958	.424638E-04
20.000000	.999954	.455061E-04

SURVIVABILITY FOR PHC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.600063E-08
2.000000	1.000000	.120024E-07
3.000000	1.000000	.180053E-07
4.000000	1.000000	.240095E-07
5.000000	1.000000	.300148E-07
6.000000	1.000000	.360214E-07
7.000000	1.000000	.420290E-07
8.000000	1.000000	.480380E-07
9.000000	1.000000	.540480E-07
10.000000	1.000000	.600593E-07
11.000000	1.000000	.660717E-07
12.000000	1.000000	.720854E-07
13.000000	1.000000	.781002E-07
14.000000	1.000000	.841162E-07
15.000000	1.000000	.901334E-07
16.000000	1.000000	.961518E-07
17.000000	1.000000	.102171E-06
18.000000	1.000000	.108192E-06
19.000000	1.000000	.114214E-06
20.000000	1.000000	.120237E-06

SURVIVABILITY FOR BETA

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.600063E-08
2.000000	1.000000	.120024E-07
3.000000	1.000000	.180053E-07
4.000000	1.000000	.240095E-07
5.000000	1.000000	.300148E-07
6.000000	1.000000	.360214E-07
7.000000	1.000000	.420290E-07
8.000000	1.000000	.480380E-07
9.000000	1.000000	.540480E-07
10.000000	1.000000	.600593E-07
11.000000	1.000000	.660717E-07
12.000000	1.000000	.720854E-07
13.000000	1.000000	.781002E-07
14.000000	1.000000	.841162E-07
15.000000	1.000000	.901334E-07
16.000000	1.000000	.961518E-07
17.000000	1.000000	.102171E-06
18.000000	1.000000	.108192E-06
19.000000	1.000000	.114214E-06
20.000000	1.000000	.120237E-06

SURVIVABILITY FOR SRTC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.600063E-08
2.000000	1.000000	.120024E-07
3.000000	1.000000	.180053E-07
4.000000	1.000000	.240095E-07
5.000000	1.000000	.300148E-07
6.000000	1.000000	.360214E-07
7.000000	1.000000	.420290E-07
8.000000	1.000000	.480380E-07
9.000000	1.000000	.540480E-07
10.000000	1.000000	.600593E-07
11.000000	1.000000	.660717E-07
12.000000	1.000000	.720854E-07
13.000000	1.000000	.781002E-07
14.000000	1.000000	.841162E-07
15.000000	1.000000	.901334E-07
16.000000	1.000000	.961518E-07
17.000000	1.000000	.102171E-06
18.000000	1.000000	.108192E-06
19.000000	1.000000	.114214E-06
20.000000	1.000000	.120237E-06

SURVIVABILITY FOR EA MOM

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.879935E-06
2.000000	.999998	.175963E-05
3.000000	.999997	.263918E-05
4.000000	.999996	.351859E-05
5.000000	.999996	.439784E-05
6.000000	.999995	.527697E-05
7.000000	.999994	.615598E-05
8.000000	.999993	.703488E-05
9.000000	.999992	.791370E-05
10.000000	.999991	.879243E-05
11.000000	.999990	.967110E-05
12.000000	.999989	.105497E-04
13.000000	.999989	.114283E-04
14.000000	.999988	.123069E-04
15.000000	.999987	.131854E-04
16.000000	.999986	.140639E-04
17.000000	.999985	.149425E-04
18.000000	.999984	.158211E-04
19.000000	.999983	.166997E-04
20.000000	.999982	.175784E-04

SURVIVABILITY FOR ASA

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.399980E-06
2.000000	.999999	.799921E-06
3.000000	.999999	.119992E-05
4.000000	.999998	.159969E-05
5.000000	.999998	.199952E-05
6.000000	.999998	.239932E-05
7.000000	.999997	.279909E-05
8.000000	.999997	.319882E-05
9.000000	.999996	.359852E-05
10.000000	.999996	.399819E-05
11.000000	.999996	.439784E-05
12.000000	.999995	.479746E-05
13.000000	.999995	.519705E-05
14.000000	.999994	.559662E-05
15.000000	.999994	.599616E-05
16.000000	.999994	.639569E-05
17.000000	.999993	.679519E-05
18.000000	.999993	.719467E-05
19.000000	.999992	.759414E-05
20.000000	.999992	.799358E-05

SURVIVABILITY FOR RGYRO

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.200759E-06
2.000000	1.000000	.402839E-06
3.000000	.999999	.606239E-06
4.000000	.999999	.810962E-06
5.000000	.999999	.101701E-05
6.000000	.999999	.122438E-05
7.000000	.999999	.143398E-05
8.000000	.999998	.164310E-05
9.000000	.999998	.185446E-05
10.000000	.999998	.206714E-05
11.000000	.999998	.228115E-05
12.000000	.999998	.249650E-05
13.000000	.999997	.271318E-05
14.000000	.999997	.293119E-05
15.000000	.999997	.315054E-05
16.000000	.999997	.337123E-05
17.000000	.999996	.359326E-05
18.000000	.999996	.381662E-05
19.000000	.999996	.404133E-05
20.000000	.999996	.426738E-05

SURVIVABILITY FOR DDU

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.225361E-06
2.000000	1.000000	.456868E-06
3.000000	.999999	.694517E-06
4.000000	.999999	.938319E-06
5.000000	.999999	.118824E-05
6.000000	.999999	.144432E-05
7.000000	.999998	.171653E-05
8.000000	.999998	.197488E-05
9.000000	.999998	.224937E-05
10.000000	.999997	.253000E-05
11.000000	.999997	.281676E-05
12.000000	.999997	.310966E-05
13.000000	.999997	.340869E-05
14.000000	.999996	.371385E-05
15.000000	.999996	.402514E-05
16.000000	.999996	.434256E-05
17.000000	.999995	.466611E-05
18.000000	.999995	.499580E-05
19.000000	.999995	.533162E-05
20.000000	.999994	.567354E-05

SURVIVABILITY FOR AVVI

MISSION TIME (HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.308344E-06
2.000000	.999999	.628078E-06
3.000000	.999999	.953199E-06
4.000000	.999999	.133170E-05
5.000000	.999999	.165559E-05
6.000000	.999998	.202086E-05
7.000000	.999998	.239750E-05
8.000000	.999997	.278552E-05
9.000000	.999997	.318491E-05
10.000000	.999996	.359567E-05
11.000000	.999996	.401779E-05
12.000000	.999996	.445128E-05
13.000000	.999995	.489613E-05
14.000000	.999995	.535234E-05
15.000000	.999994	.581990E-05
16.000000	.999994	.629882E-05
17.000000	.999993	.678909E-05
18.000000	.999993	.729070E-05
19.000000	.999992	.780367E-05
20.000000	.999992	.832797E-05

SURVIVABILITY FOR A/MI

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.381247E-06
2.000000	.999999	.779757E-06
3.000000	.999999	.119557E-05
4.000000	.999998	.162855E-05
5.000000	.999998	.207882E-05
6.000000	.999997	.254634E-05
7.000000	.999997	.303109E-05
8.000000	.999996	.353308E-05
9.000000	.999996	.405230E-05
10.000000	.999995	.458875E-05
11.000000	.999995	.514241E-05
12.000000	.999994	.571329E-05
13.000000	.999994	.630138E-05
14.000000	.999993	.690667E-05
15.000000	.999992	.752917E-05
16.000000	.999992	.816886E-05
17.000000	.999991	.882574E-05
18.000000	.999991	.949981E-05
19.000000	.999990	.101911E-04
20.000000	.999989	.108995E-04

SURVIVABILITY FOR HST

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000001	.164773E-06
2.000000	1.000000	.332855E-06
3.000000	.999999	.504245E-06
4.000000	.999999	.678944E-06
5.000000	.999999	.856950E-06
6.000000	.999999	.103826E-05
7.000000	.999999	.122298E-05
8.000000	.999999	.141081E-05
9.000000	.999998	.160294E-05
10.000000	.999998	.179658E-05
11.000000	.999998	.199443E-05
12.000000	.999998	.219557E-05
13.000000	.999998	.240003E-05
14.000000	.999997	.260778E-05
15.000000	.999997	.281885E-05
16.000000	.999997	.303321E-05
17.000000	.999997	.325088E-05
18.000000	.999997	.347185E-05
19.000000	.999996	.369612E-05
20.000000	.999996	.392369E-05

SURVIVABILITY FOR AOI

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	1.000000	.229060E-06
2.000000	1.000000	.464465E-06
3.000000	.999999	.706214E-06
4.000000	.999999	.954306E-06
5.000000	.999999	.120874E-05
6.000000	.999999	.146952E-05
7.000000	.999998	.173653E-05
8.000000	.999998	.201038E-05
9.000000	.999998	.228987E-05
10.000000	.999997	.257600E-05
11.000000	.999997	.286846E-05
12.000000	.999997	.316726E-05
13.000000	.999997	.347239E-05
14.000000	.999996	.378385E-05
15.000000	.999996	.410165E-05
16.000000	.999996	.442577E-05
17.000000	.999995	.475623E-05
18.000000	.999995	.509301E-05
19.000000	.999995	.543611E-05
20.000000	.999994	.578555E-05

SURVIVABILITY FOR PCMMU

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999996	.418423E-05
2.000000	.999990	.984181E-05
3.000000	.999983	.163689E-04
4.000000	.999974	.255613E-04
5.000000	.999964	.356166E-04
6.000000	.999953	.471295E-04
7.000000	.999940	.600968E-04
8.000000	.999925	.745147E-04
9.000000	.999910	.903795E-04
10.000000	.999892	.107687E-03
11.000000	.999874	.126434E-03
12.000000	.999853	.146617E-03
13.000000	.999832	.168231E-03
14.000000	.999809	.191274E-03
15.000000	.999784	.215741E-03
16.000000	.999758	.241629E-03
17.000000	.999731	.268933E-03
18.000000	.999702	.297651E-03
19.000000	.999672	.327778E-03
20.000000	.999641	.359312E-03

SURVIVABILITY FOR OF MDM

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.622062E-06
2.000000	.999999	.128883E-05
3.000000	.999998	.200029E-05
4.000000	.999997	.275643E-05
5.000000	.999996	.355721E-05
6.000000	.999996	.440252E-05
7.000000	.999995	.529264E-05
8.000000	.999994	.622725E-05
9.000000	.999993	.720642E-05
10.000000	.999992	.823015E-05
11.000000	.999991	.929841E-05
12.000000	.999990	.104112E-04
13.000000	.999988	.115684E-04
14.000000	.999987	.127701E-04
15.000000	.999986	.140163E-04
16.000000	.999985	.153069E-04
17.000000	.999983	.166419E-04
18.000000	.999982	.180213E-04
19.000000	.999981	.194451E-04
20.000000	.999979	.209132E-04

SURVIVABILITY FOR 04 MOM

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.622062E-06
2.000000	.999999	.123883E-05
3.000000	.999998	.200029E-05
4.000000	.999997	.275643E-05
5.000000	.999996	.355721E-05
6.000000	.999996	.440252E-05
7.000000	.999995	.529264E-05
8.000000	.999994	.622725E-05
9.000000	.999993	.720642E-05
10.000000	.999992	.823015E-05
11.000000	.999991	.929841E-05
12.000000	.999990	.104112E-04
13.000000	.999988	.115684E-04
14.000000	.999987	.127701E-04
15.000000	.999986	.140163E-04
16.000000	.999985	.153069E-04
17.000000	.999983	.166419E-04
18.000000	.999982	.180213E-04
19.000000	.999981	.194451E-04
20.000000	.999979	.209132E-04

SURVIVABILITY FOR AFT FC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.143325E-05
2.000000	.999997	.289090E-05
3.000000	.999996	.437307E-05
4.000000	.999994	.587988E-05
5.000000	.999993	.741146E-05
6.000000	.999991	.895793E-05
7.000000	.999989	.105494E-04
8.000000	.999988	.121561E-04
9.000000	.999986	.137879E-04
10.000000	.999985	.154452E-04
11.000000	.999983	.171280E-04
12.000000	.999981	.188365E-04
13.000000	.999979	.205707E-04
14.000000	.999978	.223308E-04
15.000000	.999976	.241168E-04
16.000000	.999974	.259291E-04
17.000000	.999972	.277675E-04
18.000000	.999970	.296324E-04
19.000000	.999968	.315238E-04
20.000000	.999967	.334417E-04

SURVIVABILITY FOR S CPIT

MISSION TIME (HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999989	.113743E-04
2.000000	.999976	.235774E-04
3.000000	.999963	.366292E-04
4.000000	.999949	.505495E-04
5.000000	.999935	.653591E-04
6.000000	.999919	.810744E-04
7.000000	.999902	.977179E-04
8.000000	.999885	.115399E-03
9.000000	.999866	.133864E-03
10.000000	.999847	.153404E-03
11.000000	.999826	.173940E-03
12.000000	.999804	.195516E-03
13.000000	.999782	.218124E-03
14.000000	.999759	.241792E-03
15.000000	.999733	.266537E-03
16.000000	.999708	.292380E-03
17.000000	.999681	.319337E-03
18.000000	.999653	.347427E-03
19.000000	.999623	.376667E-03
20.000000	.999593	.407075E-03

SURVIVABILITY FOR M CPIT

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999963	.163026E-04
2.000000	.999964	.359956E-04
3.000000	.999942	.575979E-04
4.000000	.999918	.816224E-04
5.000000	.999892	.108086E-03
6.000000	.999863	.137004E-03
7.000000	.999832	.168392E-03
8.000000	.999798	.202266E-03
9.000000	.999761	.238641E-03
10.000000	.999722	.277531E-03
11.000000	.999681	.318952E-03
12.000000	.999637	.362919E-03
13.000000	.999591	.409446E-03
14.000000	.999541	.458548E-03
15.000000	.999489	.510240E-03
16.000000	.999435	.564535E-03
17.000000	.999379	.621448E-03
18.000000	.999319	.680993E-03
19.000000	.999257	.743184E-03
20.000000	.999192	.808035E-03

SURVIVABILITY FOR FT DTS

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.133823E-05
2.000000	.999997	.277977E-05
3.000000	.999996	.432455E-05
4.000000	.999994	.597252E-05
5.000000	.999992	.772360E-05
6.000000	.999990	.957776E-05
7.000000	.999988	.1153495-04
8.000000	.999986	.135950E-04
9.000000	.999984	.157580E-04
10.000000	.999982	.180238E-04
11.000000	.999980	.203923E-04
12.000000	.999977	.228636E-04
13.000000	.999975	.254374E-04
14.000000	.999972	.281139E-04
15.000000	.999969	.3089286-04
16.000000	.999966	.3377436-04
17.000001	.999963	-.367581E-04
18.000000	.999960	.398442E-04
19.000000	.999957	.430326E-04
20.000000	.999954	.463232E-04

SURVIVABILITY FOR FWD FC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999992	.793492E-05
2.000000	.999983	.165544E-04
3.000000	.999974	.258684E-04
4.000000	.999964	.358868E-04
5.000000	.999953	.466195E-04
6.000000	.999942	.580763E-04
7.000000	.999930	.702568E-04
8.000000	.999917	.832006E-04
9.000000	.999903	.968872E-04
10.000000	.999889	.111336E-03
11.000000	.999873	.126557E-03
12.000000	.999857	.142558E-03
13.000000	.999841	.159349E-03
14.000000	.999823	.175940E-03
15.000000	.999805	.193339E-03
16.000000	.999785	.214555E-03
17.000000	.999765	.234598E-03
18.000000	.999745	.255475E-03
19.000000	.999723	.277196E-03
20.000000	.999700	.299769E-03

THIS PAGE INTENTIONALLY LEFT BLANK

6.3 SELECTED SYSTEM OPTIONS

6.3.1 USE OF ALTERNATE MDM PORT

The first option is to reconfigure GPC bus assignments to use the alternate flight critical MDM ports. This prevents the loss of an MDM due to a failure of the MIA, A/D, or SCU portions of the MDM. The effect of this is to internally duplex that portion of these MDM modules. The failure probability of an internally duplexed module is approximately

$$F(T) = (\lambda T)^2$$

This is a very good approximation for $\lambda T < .01$. The failure rate of these MDM submodules is 74 per 10^6 hours. So for a six-hour mission, λT becomes $.00148 << .01$, and $F(T)$ is $2.19(10)^{-6}$. If we divide $F(T)$ by 20 hours, we have an effective failure rate of .11 failures per 10^6 hours, certainly very small compared to the remaining MDM failure rate. So for mission times less than 20 hours, we can neglect the failure rate of the MIA, A/D, and SCU when we use the alternate port.

For the purpose of illustration, we assume the four GPCs have access to the alternate aft flight critical MDM ports. This is true of OFT, but not for ALT. The results for a six-hour mission are summarized on the opposite page. Five pages of printouts of the results for 1 to 20 hour mission times follow. There is considerable improvement in the individual MDM and aft flight critical failure probabilities, but very little improvement in the forward flight critical. As the baseline failure rates stand, there is little to be gained from this option. But if the TACAN and MSBLS failure rates are overly pessimistic, this option should be studied further.

UNIT	FAILURE PROBABILITY	
	WITH ALTERNATE PORT	WITHOUT ALTERNATE PORT
FWD MDM	$3.7(10)^{-6}$	$5.5(10)^{-6}$
AFT MDM	$3.5(10)^{-6}$	$5.3(10)^{-6}$
FWD Flight Critical	$5.5(10)^{-5}$	$5.8(10)^{-5}$
AFT Flight Critical	$7.0(10)^{-6}$	$9.0(10)^{-6}$
Safety Critical	$7.6(10)^{-5}$	$8.1(10)^{-5}$

SUMMARY OF THE ALTERNATE MDM PORT OPTION

SURVIVABILITY FOR FF NOM

MISSION TIME (HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.623952E-06
2.000000	.999999	.124781E-05
3.000000	.999998	.187158E-05
4.000000	.999998	.249527E-05
5.000000	.999997	.311887E-05
6.000000	.999996	.374241E-05
7.000000	.999996	.436587E-05
8.000000	.999995	.498927E-05
9.000000	.999994	.561260E-05
10.000000	.999994	.623588E-05
11.000000	.999993	.685911E-05
12.000000	.999993	.748229E-05
13.000000	.999992	.810543E-05
14.000000	.999991	.872853E-05
15.000000	.999991	.935159E-05
16.000000	.999990	.997463E-05
17.000000	.999989	.105976E-04
18.000000	.999989	.112206E-04
19.000000	.999988	.118436E-04
20.000000	.999988	.124665E-04

SURVIVABILITY FOR FA MOM

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.583958E-06
2.000000	.999999	.116793E-05
3.000000	.999998	.175163E-05
4.000000	.999998	.233536E-05
5.000000	.999997	.291901E-05
6.000000	.999996	.350260E-05
7.000000	.999996	.408612E-05
8.000000	.999995	.466958E-05
9.000000	.999995	.525299E-05
10.000000	.999994	.583635E-05
11.000000	.999994	.641966E-05
12.000000	.999993	.700292E-05
13.000000	.999992	.758615E-05
14.000000	.999992	.816934E-05
15.000000	.999991	.875249E-05
16.000000	.999991	.933562E-05
17.000000	.999990	.991872E-05
18.000000	.999989	.105018E-04
19.000000	.999989	.110849E-04
20.000000	.999988	.116679E-04

SURVIVABILITY FOR FWD FC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999992	.759245E-05
2.000000	.999984	.157750E-04
3.000000	.999975	.245557E-04
4.000000	.999966	.339426E-04
5.000000	.999956	.439435E-04
6.000000	.999945	.545663E-04
7.000000	.999934	.658187E-04
8.000000	.999922	.777084E-04
9.000000	.999910	.902431E-04
10.000000	.999897	.103430E-03
11.000000	.999883	.117279E-03
12.000000	.999868	.131793E-03
13.000000	.999853	.146983E-03
14.000000	.999837	.162855E-03
15.000000	.999821	.179417E-03
16.000000	.999803	.196676E-03
17.000000	.999785	.214640E-03
18.000000	.999767	.233314E-03
19.000000	.999747	.252707E-03
20.000000	.999727	.272825E-03

SURVIVABILITY FOR AFT FC

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999999	.113178E-05
2.000000	.999998	.227696E-05
3.000000	.999997	.343559E-05
4.000000	.999995	.460772E-05
5.000000	.999994	.579341E-05
6.000000	.999993	.699271E-05
7.000000	.999992	.820563E-05
8.000000	.999991	.943236E-05
9.000000	.999989	.106728E-04
10.000000	.999988	.119271E-04
11.000000	.999987	.131953E-04
12.000000	.999986	.144773E-04
13.000000	.999984	.157734E-04
14.000000	.999983	.170835E-04
15.000000	.999982	.184077E-04
16.000000	.999980	.197461E-04
17.000000	.999979	.210986E-04
18.000000	.999978	.224654E-04
19.000000	.999976	.238465E-04
20.000000	.999975	.252419E-04

SURVIVABILITY FOR S CRIT

MISSION TIME(HOURS)	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
1.000000	.999989	.107304E-04
2.000000	.999978	.221841E-04
3.000000	.999965	.343791E-04
4.000000	.999953	.473332E-04
5.000000	.999939	.610641E-04
6.000000	.999924	.755894E-04
7.000000	.999909	.909264E-04
8.000000	.999893	.107093E-03
9.000000	.999876	.124105E-03
10.000000	.999858	.141982E-03
11.000000	.999839	.160738E-03
12.000000	.999820	.180393E-03
13.000000	.999799	.200962E-03
14.000000	.999778	.222461E-03
15.000000	.999755	.244909E-03
16.000000	.999732	.268321E-03
17.000000	.999707	.292713E-03
18.000000	.999682	.318103E-03
19.000000	.999655	.344505E-03
20.000000	.999628	.371937E-03

6.3.2 TRANSIENT-FAULT RECOVERY OPTIONS

The baseline transient-fault recovery option, which is a delay before attempting a permanent-fault recovery, is quite effective for transient faults occurring external to the GPCs. This is due to the filtering of the processing algorithms and the slow response time of the actuators and displays. This recovery method is not as effective for transients within the GPC. It is easy for a program to be altered by a memory transient during a restore cycle. Also, CPU and IOP transients can alter data. Thus, a GPC can be left with a "permanent" fault actually resulting from a transient.

The three alternate transient-fault recovery options studied here are rollback, rollahead, and a combination of rollahead and memory copy. Rollback is defined as the procedure where the current program segment is rerun following fault detection. Rollahead is defined as the procedure where the fault-free GPCs pass the current machine-state and data points to the indicated faulty machine and continue computation. Memory copy is the procedure where the contents of the memories of the good GPCs are passed to the faulty GPC at a low duty cycle on a cycle-stealing basis. Memory copy is followed by a rollahead after completion to bring the faulty GPC on line.

The effectiveness of each of the transient recovery options is generated by the simulator. The simulation provides the transient leakage parameter for the model. Since transient-fault parameters for the Shuttle GPCs have not been established, the model results are given for a wide range of transient environments. The baseline GPC transient rate was made equal to the permanent, i.e., τ/λ is unity. The results presented in the printouts that follow, in the case of the delay recovery option, show the results of considering both more hostile ($\tau/\lambda>1$) and more benign ($\tau/\lambda<1$) transient environments.

The transient recovery options results are summarized on the opposite page. Table 6.3-I lists the options and the resulting transient leakages. Delay recovery exhibits the highest leakage except for the case of rollahead and memory copy with two GPCs remaining, where these recovery options are not applicable. Memory copy has the best leakage because memory transients are corrected. Figure 6.3-1 illustrates how these differences become amplified in a hostile transient environment. Listings of the complete results are presented on the following eight pages. They are denoted Tables 6.3-II through 6.3-IX.

TABLE 6.3-I LEAKAGE RESULTS FOR TRANSIENT RECOVERY OPTIONS

OPTION	TRANSIENT LEAKAGE		
	4 GPCs	3 GPCs	2 GPCs
Delay Recovery	.703	.703	.703
Rollback	.403	.403	.403
Rollahead	.398	.398	1
Memory Copy	0	0	1

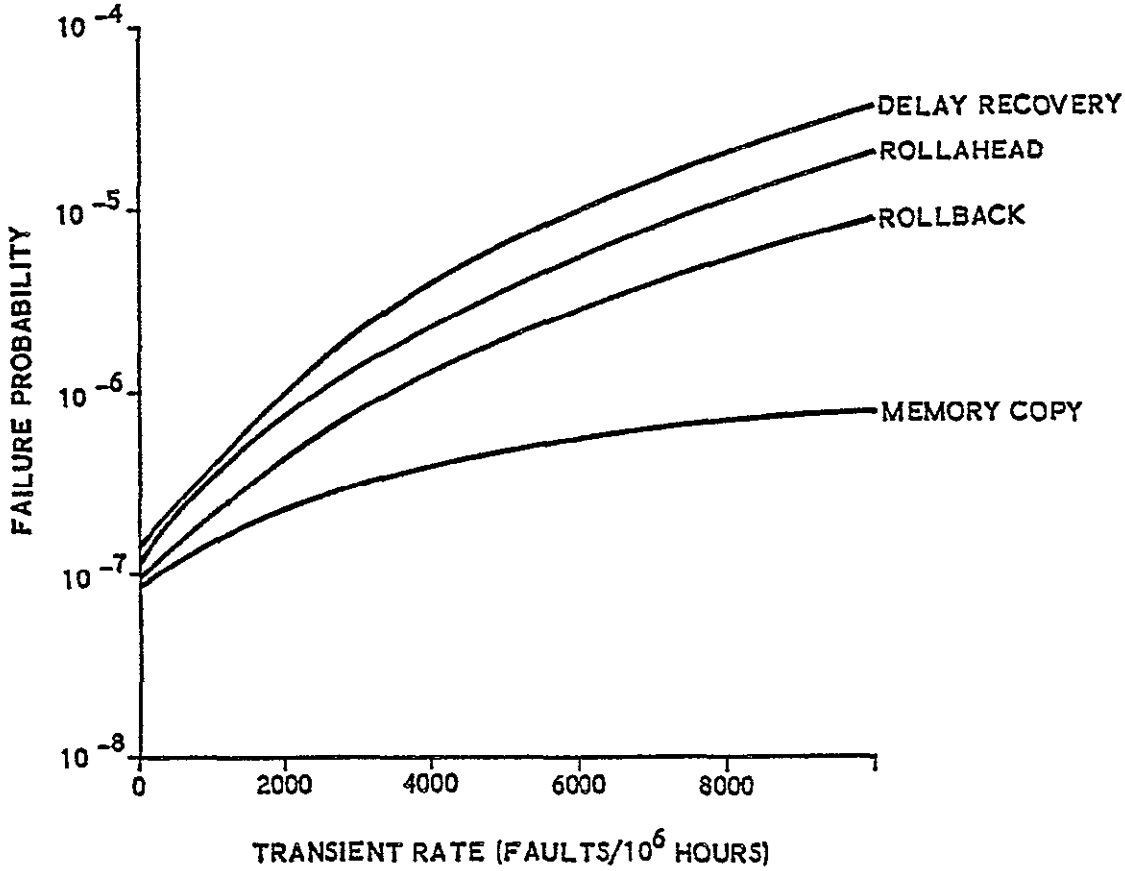


FIGURE 6.3-1 FAILURE PROBABILITY RESULTS FOR VARIOUS TRANSIENT RECOVERY OPTIONS AND TRANSIENT FAULT RATES

TABLE 6.3-II VARIATIONS IN TRANSIENT FAULT RATE FOR THE DELAY RECOVERY TRANSIENT RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .500000CE+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999999	.7248427E-07
.000100	.9999999	.9894629E-07
.000200	.9999999	.1077165E-06
.000300	.9999999	.1289433E-06
.000400	.9999998	.1527744E-06
.000500	.9999998	.1793567E-06
.000600	.9999998	.2088369E-06
.000700	.9999998	.2413609E-06
.000800	.9999997	.2770742E-06
.000900	.9999997	.3161216E-06
.001000	.9999996	.3586473E-06

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999192	.8079221E-04
.000100	.9999192	.8090867E-04
.000200	.9999192	.8082744E-04
.000300	.9999192	.8084866E-04
.000400	.9999191	.8087249E-04
.000500	.9999191	.8089907E-04
.000600	.9999191	.8092855E-04
.000700	.9999190	.8096107E-04
.000800	.9999190	.8099678E-04
.000900	.9999190	.8103583E-04
.001000	.9999189	.8107835E-04

TABLE 6.3-III VARIATIONS IN TRANSIENT FAULT RATE FOR THE DELAY RECOVERY TRANSIENT RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999996	.3586473E-06
.002000	.9999993	.1006559E-05
.003000	.9999978	.2156908E-05
.004000	.9999961	.3944939E-05
.005000	.9999935	.6500595E-05
.006000	.9999901	.9948654E-05
.007000	.9999856	.1440886E-04
.008000	.9999809	.1999606E-04
.009000	.9999732	.2682033E-04
.010000	.9999650	.3498710E-04

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999184	.8159043E-04
.002000	.9999178	.8223829E-04
.003000	.9999166	.8338855E-04
.004000	.9999148	.8517643E-04
.005000	.9999127	.8773188E-04
.006000	.9999098	.9117966E-04
.007000	.9999044	.9563950E-04
.008000	.9998988	.1012263E-03
.009000	.9998920	.1080500E-03
.010000	.9998838	.1162161E-03

TABLE 6.3-IV VARIATIONS IN TRANSIENT FAULT RATE FOR THE ROLLAHEAD RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999999	.7248427E-07
.000100	.9999999	.8627534E-07
.000200	.9999999	.1015241E-06
.000300	.9999999	.1182983E-06
.000400	.9999999	.1366650E-06
.000500	.9999998	.1566914E-06
.000600	.9999998	.1784445E-06
.000700	.9999998	.2019908E-06
.000800	.9999998	.2273969E-06
.000900	.9999997	.2547294E-06
.001000	.9999997	.2840540E-06

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999187	.8130429E-04
.000100	.9999187	.8131808E-04
.000200	.9999187	.8133333E-04
.000300	.9999186	.8135010E-04
.000400	.9999186	.8136847E-04
.000500	.9999186	.8138849E-04
.000600	.9999186	.8141024E-04
.000700	.9999186	.8143379E-04
.000800	.9999185	.8145919E-04
.000900	.9999185	.8148652E-04
.001000	.9999185	.8151585E-04

TABLE 6.3-V VARIATIONS IN TRANSIENT FAULT RATE FOR THE ROLLAHEAD RECOVERY METHOD

CARRYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999997	.2840540E-06
.002000	.9999997	.7012847E-06
.003000	.9999986	.1389054E-05
.004000	.9999976	.2410340E-05
.005000	.9999962	.3826260E-05
.006000	.9999947	.5696104E-05
.007000	.9999919	.8077374E-05
.008000	.9999890	.1102581E-04
.009000	.9999854	.1459545E-04
.010000	.9999812	.1883862E-04

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999185	.8151595E-04
.002000	.9999181	.8193304E-04
.003000	.9999174	.8262076E-04
.004000	.9999164	.8364196E-04
.005000	.9999140	.8505776E-04
.006000	.9999131	.8692746E-04
.007000	.9999107	.8930853E-04
.008000	.9999077	.9225673E-04
.009000	.9999042	.9582608E-04
.010000	.9999990	.1000689E-03

TABLE 6.3-VI VARIATIONS IN TRANSIENT FAULT RATE WITH THE MEMORY COPY RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999999	.7248427E-07
.000100	.9999999	.7977431E-07
.000200	.9999999	.8706095E-07
.000300	.9999999	.9434278E-07
.000400	.9999999	.1016203E-06
.000500	.9999999	.1088950E-06
.000600	.9999999	.1161622E-06
.000700	.9999999	.1234268E-06
.000800	.9999999	.1306871E-06
.000900	.9999999	.1379430E-06
.001000	.9999999	.1451954E-06

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999187	.8130429E-04
.000100	.9999187	.8131158E-04
.000200	.9999187	.8131887E-04
.000300	.9999187	.8132615E-04
.000400	.9999187	.8133343E-04
.000500	.9999187	.8134070E-04
.000600	.9999187	.8134797E-04
.000700	.9999186	.8135523E-04
.000800	.9999186	.8136249E-04
.000900	.9999186	.8136975E-04
.001000	.9999186	.8137700E-04

TABLE 6.3-VII VARIATIONS IN TRANSIENT FAULT RATE WITH THE MEMORY COPY RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .5000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999999	.1451954E-06
.002000	.9999998	.2174736E-06
.003000	.9999997	.2893246E-06
.004000	.9999996	.3607505E-06
.005000	.9999996	.4317544E-06
.006000	.9999995	.5023394E-06
.007000	.9999994	.5725084E-06
.008000	.9999994	.6422643E-06
.009000	.9999993	.7116102E-06
.010000	.9999992	.7805488E-06

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999186	.8137700E-04
.002000	.9999186	.8144927E-04
.003000	.9999185	.8152112E-04
.004000	.9999184	.8159254E-04
.005000	.9999183	.8166353E-04
.006000	.9999183	.8173411E-04
.007000	.9999182	.8180428E-04
.008000	.9999181	.8187403E-04
.009000	.9999181	.8194337E-04
.010000	.9999180	.8201230E-04

TABLE 6.3-VIII VARIATIONS IN TRANSIENT FAULT RATE WITH THE ROLLBACK RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999999	.7248427E-07
.000100	.9999999	.8164759E-07
.000200	.9999999	.9154864E-07
.000300	.9999999	.1022154E-06
.000400	.9999999	.1136759E-06
.000500	.9999999	.1259579E-06
.000600	.9999999	.1390892E-06
.000700	.9999999	.1530977E-06
.000800	.9999998	.1680110E-06
.000900	.9999998	.1838567E-06
.001000	.9999998	.2006624E-06

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
0.000000	.9999187	.8130429E-04
.000100	.9999187	.8131346E-04
.000200	.9999187	.8132336E-04
.000300	.9999187	.8133402E-04
.000400	.9999187	.8134548E-04
.000500	.9999186	.8135776E-04
.000600	.9999186	.8137089E-04
.000700	.9999186	.8138490E-04
.000800	.9999186	.8139981E-04
.000900	.9999186	.8141566E-04
.001000	.9999186	.8143246E-04

TABLE 6.3-IX VARIATIONS IN TRANSIENT FAULT RATE WITH THE ROLLBACK RECOVERY METHOD

VARYING UNIT IS GPC

MISSION TIME IS .6000000E+01 HOURS

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999998	.2006624E-06
.002000	.9999996	.4275409E-06
.003000	.9999992	.7802943E-06
.004000	.9999987	.1285497E-05
.005000	.9999980	.1969131E-05
.006000	.9999971	.2856598E-05
.007000	.9999960	.3972723E-05
.008000	.9999947	.5341768E-05
.009000	.9999930	.6987436E-05
.010000	.9999911	.8932883E-05

SAFETY CRITICAL SURVIVABILITY

TAU	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.001000	.9999186	.8143246E-04
.002000	.9999183	.8165932E-04
.003000	.9999180	.8201859E-04
.004000	.9999175	.8251721E-04
.005000	.9999168	.8320079E-04
.006000	.9999159	.8409818E-04
.007000	.9999148	.8520421E-04
.008000	.9999134	.8657315E-04
.009000	.9999118	.8821868E-04
.010000	.9999098	.9016397E-04

6.3.3 VARIATIONS IN THE DETECTABILITY PREDICTION

In the baseline parameter set, the GPC detectability is chosen to be one because no uncoverage has been identified by the manufacturer. However, there is a 1-out-of-2^{32} chance that a set of incorrect computations sums to the correct result for the output comparison. Thus, it is of interest to obtain results for GPC detectability values other than unity. The detectability for devices where a coverage analysis was unavailable was chosen to be .999, i.e., the design goal value. This section presents the results of an examination of the effects of imperfect GPC detectability and what happens if .999 is too pessimistic for the peripheral devices.

Table 6.3-X summarizes the effects of imperfect GPC detectability. We feel that the cooperative detection techniques used by the GPCs achieves a detectability of at least .999 99. This results in more than a three-fold degradation of the estimated GPC survivability from that estimated for unity detectability, but it doesn't affect the overall safety-critical survivability. A GPC detectability of .999 is shown for completeness. The resulting increase in GPC and safety-critical failure probability is dramatic.

The next question is what is to be gained by improving the flight-critical device detectabilities. In Table 6.3-XII, TACAN detectability is varied from .999 to .999 9. This results in a three-fold gain in TACAN survivability and a gain from $7.7(10)^{-5}$ to $5.6(10)^{-5}$ in safety-critical failure probability. Further increases in TACAN detectability add little to the safety-critical survivability.

Next, it is appropriate to ask what happens if all the devices detectabilities are improved. Table 6.3-XI summarizes the improvements achieved in this case. Safety-critical failure probability has achieved nearly a four-fold improvement by increasing the device detectability from .999 to .9999. Further improvements bring smaller gains.

TABLE 6.3-X FAILURE PROBABILITIES FOR IMPERFECT GPC DETECTABILITY

GPC DETECTABILITY	FAILURE PROBABILITY	
	GPC	SAFETY-CRITICAL
.999,999,999	$1.8(10)^{-7}$	$8.2(10)^{-5}$
.999,999,9	$1.8(10)^{-7}$	$8.2(10)^{-5}$
.999,99	$6.5(10)^{-7}$	$8.2(10)^{-5}$
.999	$4.8(10)^{-5}$	$1.0(10)^{-4}$

TABLE 6.3-XI FAILURE PROBABILITIES FOR IMPROVEMENTS IN DETECTABILITY FOR ALL DEVICES

DETECTABILITY FOR EVERY DEVICE	FAILURE PROBABILITY			
	TACAN	MSBLS	FLIGHT-FORWARD	SAFETY-CRITICAL
.999	$2.3(10)^{-5}$	$1.0(10)^{-5}$	$5.8(10)^{-5}$	$8.1(10)^{-5}$
.999,9	$7.3(10)^{-6}$	$2.3(10)^{-6}$	$1.7(10)^{-5}$	$2.2(10)^{-5}$
.999,99	$5.7(10)^{-6}$	$1.5(10)^{-6}$	$1.4(10)^{-5}$	$1.7(10)^{-5}$
.999,999	$5.6(10)^{-6}$	$1.4(10)^{-6}$	$1.3(10)^{-5}$	$1.6(10)^{-5}$

TABLE 6.3-XII SIX HOUR SURVIVABILITY FOR INCREASES IN TACAN DETECTABILITY

VARYING UNIT IS TACAN

MISSION TIME IS .6000000E+01 HOURS

DETECTABILITY THREE	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.999000	.9999765	.2348436E-04
.999100	.9999783	.2170103E-04
.999200	.9999801	.1991770E-04
.999300	.9999819	.1813437E-04
.999400	.9999836	.1635104E-04
.999500	.9999854	.1456770E-04
.999600	.9999872	.1278437E-04
.999700	.9999890	.1100104E-04
.999800	.9999908	.9217709E-05
.999900	.9999926	.7434377E-05
1.000000	.9999943	.5651045E-05

SAFETY CRITICAL SURVIVABILITY

DETECTABILITY THREE	CONFIGURATION SURVIVABILITY	FAILURE PROBABILITY
.999000	.9999228	.7722200E-04
.999100	.9999246	.7544488E-04
.999200	.9999263	.7366776E-04
.999300	.9999281	.7189064E-04
.999400	.9999299	.7011352E-04
.999500	.9999317	.6833641E-04
.999600	.9999334	.6655929E-04
.999700	.9999352	.6478217E-04
.999800	.9999370	.6300505E-04
.999900	.9999388	.6122793E-04
1.000000	.9999405	.5945081E-04

TABLE 6.3-XIII SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 999 999

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCDS	.9999947	.5329936E-05
GPC	.9999999	.6290993E-07
FF MDM	.9999945	.5516707E-05
ADTA	.9999940	.5996164E-05
ACCEL	.9999980	.2044755E-05
IMU	.9999944	.5587907E-05
TACAN	.9999765	.2348436E-04
MSBLS	.9999896	.1035253E-04
PHC	1.0000000	.3602135E-07
RDTA	1.0000000	.3602135E-07
SPTC	1.0000000	.3602135E-07
FA MDM	.9999947	.5276966E-05
ASA	.9999976	.2399321E-05
RGYRO	.9999988	.1224380E-05
DDU	.9999986	.1444317E-05
AVVI	.9999980	.2020859E-05
A/MI	.9999975	.2546337E-05
HSI	.9999990	.1038263E-05
ADI	.9999985	.1469515E-05
PCMMU	.9999529	.4712953E-04
OF MDM	.9999928	.7206424E-05
OA MDM	.9999928	.7206424E-05
AFT FC	.9999911	.8901980E-05
S CRIT	.9999184	.8158558E-04
M CRIT	.9998569	.1431222E-03
FT DIS	.9999904	.9577756E-05
FWD FC	.9999423	.5771456E-04

TABLE 6.3-XIV SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 999 9

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCOS	.9999947	.5329936E-05
GPC	.9999999	.6667941E-07
FF MDM	.9999945	.5516707E-05
ADTA	.9999940	.5996164E-05
ACCEL	.9999980	.2044755E-05
IMU	.9999944	.5587907E-05
TACAN	.9999765	.2348436E-04
MSBLS	.9999896	.1035253E-04
PHC	1.0000000	.3602135E-07
PPTA	1.0000000	.3602135E-07
SPTC	1.0000000	.3602135E-07
FA MDM	.9999947	.5276966E-05
ASA	.9999976	.2399321E-05
RGYRO	.9999988	.1224380E-05
PDU	.9999986	.1444317E-05
AVVI	.9999980	.2020859E-05
A/MI	.9999975	.2546337E-05
HSI	.9999990	.1038263E-05
ADI	.9999985	.1469515E-05
PCMMU	.9999529	.4712953E-04
OF MDM	.9999928	.7206424E-05
OA MDM	.9999928	.7206424E-05
AFT FC	.9999911	.8901980E-05
S CRIT	.9999184	.8158935E-04
M CRIT	.9998569	.1431260E-03
FT DIS	.9999904	.9577756E-05
FWD FC	.9999423	.5771456E-04

TABLE 6.3-XV SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999 99

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCDS	.9999947	.5329936E-05
GPC	.9999996	.4436273E-06
FF MDM	.9999945	.5516707E-05
ADTA	.9999940	.5996164E-05
ACCEL	.9999980	.2044755E-05
IMU	.9999944	.5587907E-05
TACAN	.9999765	.2348436E-04
MSBLS	.9999896	.1035253E-04
RHC	1.0000000	.3602135E-07
RPTA	1.0000000	.3602135E-07
SPTC	1.0000000	.3602135E-07
FA MDM	.9999947	.5276966E-05
ASA	.9999976	.2399321E-05
RGYRO	.9999988	.1224380E-05
DDU	.9999986	.1444317E-05
AVVI	.9999980	.2020859E-05
A/MI	.9999975	.2546337E-05
HSI	.9999990	.1038263E-05
ADI	.9999985	.1469515E-05
PCMMU	.9999529	.4712953E-04
OF MDM	.9999928	.7206424E-05
CA MDM	.9999928	.7206424E-05
AFT FC	.9999911	.8901980E-05
S CRIT	.9999180	.8196627E-04
M CRIT	.9998565	.1435029E-03
FT DIS	.9999904	.9577756E-05
FWD FC	.9999423	.5771456E-04

TABLE 6.3-XVI SIX HOUR SURVIVABILITIES WHEN GPC DETECTABILITY IS .999

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCOS	.9999947	.5329936E-05
GPC	.9999524	.4755363E-04
FF MDM	.9999945	.5516707E-05
ADTA	.9999940	.5996164E-05
ACCEL	.9999980	.2044755E-05
IMU	.9999944	.5587907E-05
TACAN	.9999999	.7214457E-07
MSBLS	.9999896	.1035253E-04
RHC	1.0000000	.3602135E-07
RPTA	1.0000000	.3602135E-07
SBTC	1.0000000	.3602135E-07
FA MDM	.9999947	.5276966E-05
ASA	.9999976	.2399321E-05
RGYRO	.9999988	.1224380E-05
DDU	.9999986	.1444317E-05
AVVI	.9999980	.2020859E-05
A/MI	.9999975	.2546337E-05
HSI	.9999990	.1038263E-05
ADI	.9999985	.1469515E-05
PCMMU	.9999529	.4712953E-04
OF MDM	.9999928	.7206424E-05
OA MDM	.9999928	.7206424E-05
AFT FC	.9999911	.8901980E-05
S CRIT	.9998967	.1033202E-03
M CRIT	.9998351	.1648555E-03
FT DIS	.9999904	.9577756E-05
FHO FC	.9999680	.3196053E-04

TABLE 6.3-XVII SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 9

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCDS	.9999990	.1014979E-05
GPC	.9999996	.3546683E-06
FF MDM	.9999994	.5521464E-06
ADTA	.9999994	.6002274E-06
ACCEL	.9999997	.2634626E-06
IMU	.9999990	.9594941E-06
TACAN	.9999927	.7343147E-05
MSRLS	.9999977	.2267179E-05
RHC	1.0000000	.3621601E-08
RPTA	1.0000000	.3621601E-08
SBTC	1.0000000	.3621601E-08
FA MDM	.9999995	.5281129E-06
ASA	.9999998	.2399712E-06
RGYRO	.9999999	.1441000E-06
ODU	.9999998	.1779385E-06
AVVI	.9999997	.2969821E-06
A/MI	.9999996	.4242761E-06
HSI	.9999999	.1088544E-06
ADI	.9999998	.1826476E-06
PCMMU	.9998697	.1302685E-03
OF MDM	.9999810	.1896295E-04
OA MDM	.9999810	.1896295E-04
AFT FC	.9999987	.1300337E-05
S CRIT	.9999779	.2209754E-04
M CRIT	.9998097	.1902829E-03
FT DIS	.9999977	.2254238E-05
FWD FC	.9999828	.1717341E-04

TABLE 6.3-XVIII SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 99

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCDS	.9999993	.6553418E-06
GPC	.9999996	.3546683E-06
FF MDM	.9999999	.5568932E-07
ADTA	.9999999	.6063254E-07
ACCEL	.9999999	.8533318E-07
IMU	.9999995	.4966521E-06
TACAN	.9999943	.5729017E-05
MSBLS	.9999985	.1458642E-05
RHC	1.0000000	.3816183E-09
RPTA	1.0000000	.3816183E-09
SBTC	1.0000000	.3816183E-09
FA MDM	.9999999	.5322666E-07
ASA	1.0000000	.2403605E-07
RGYRO	1.0000000	.3607195E-07
DDU	.9999999	.1179205E-06
AVVI	.9999998	.2152818E-06
A/HI	.9999997	.3237044E-06
HSI	.9999999	.6480658E-07
ADI	.9999999	.1216586E-06
PCMMU	.9998706	.1293540E-03
OF MDM	.9999812	.1880278E-04
OA MDM	.9999812	.1880278E-04
AFT FC	.9999995	.5335751E-06
S CRIT	.9999835	.1653373E-04
M CRIT	.9998165	.1834853E-03
FT DIS	.9999981	.1907151E-05
FWD FC	.9999869	.1308304E-04

TABLE 6.3-XIX SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 999

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCDS	.9999994	.6193781E-06
GPC	.9999996	.3546683E-06
FF MDM	1.0000000	.6043571E-08
ADTA	1.0000000	.6673055E-08
ACCEL	.9999999	.6752025E-07
IMU	.9999995	.4503679E-06
TACAN	.9999944	.5567604E-05
MSBLS	.9999986	.1377788E-05
RHC	1.0000000	.5761791E-10
RPTA	1.0000000	.5761791E-10
SBTC	1.0000000	.5761791E-10
FA MDM	1.0000000	.5738038E-08
ASA	1.0000000	.2442555E-08
RGYRO	1.0000000	.2526914E-07
DDU	.9999999	.1119187E-06
AVVI	.9999998	.2071117E-06
A/MI	.9999997	.3136473E-06
HSI	.9999999	.6040180E-07
ADI	.9999999	.1155597E-06
PCMMU	.9998707	.1292625E-03
OF MDM	.9999812	.1878677E-04
OA MDM	.9999812	.1878677E-04
AFT FC	.9999995	.4568989E-06
S CRIT	.9999840	.1597734E-04
M CRIT	.9998172	.1828055E-03
FT DIS	.9999981	.1872442E-05
FWD FC	.9999873	.1267400E-04

TABLE 6.3-XX SIX HOUR SURVIVABILITIES WHEN PERIPHERAL DETECTABILITIES ARE .999 999 9

MISSION TIME IS .6000000E+01 HOURS

UNIT NAME	BASELINE SURVIVABILITY	FAILURE PROBABILITY
MCOS	.9999994	.6157817E-06
GPC	.9999996	.3546683E-06
FF MDM	1.0000000	.1079030E-08
ADTA	1.0000000	.1277073E-08
ACCEL	.9999999	.6573895E-07
IMU	.9999996	.4457395E-06
TACAN	.9999944	.5551462E-05
MSBLS	.9999986	.1369702E-05
RHC	1.0000000	.2523137E-10
RPTA	1.0000000	.2523137E-10
SBTC	1.0000000	.2523137E-10
FA MDM	1.0000000	.9891608E-09
ASA	1.0000000	.2831939E-09
RGYRO	1.0000000	.2418886E-07
DDU	.9999999	.1113185E-06
AVVI	.9999998	.2062947E-06
A/MI	.9999997	.3126416E-06
HSI	.9999999	.5996132E-07
ADI	.9999999	.1149498E-06
PCMMU	.9998707	.1292534E-03
OF MDM	.9999812	.1878517E-04
OA MDM	.9999812	.1878517E-04
AFT FC	.9999996	.4492313E-06
S CRIT	.9999841	.1592170E-04
M CRIT	.9998173	.1827376E-03
FT DIS	.9999981	.1868972E-05
FWD FC	.9999874	.1263310E-04

THIS PAGE INTENTIONALLY LEFT BLANK

6.4 SUGGESTED IMPROVEMENTS

The Shuttle orbiter avionics system was designed using the discrete fault tolerance criterion. Namely, the DPS can tolerate two faults (FO/FS) with a coverage of .999. This provides a feeling of confidence to the user of the orbiter. The other major fault tolerance criterion for system design is the survivability (or reliability or mission success probability). The frequent goal using this criterion is a balanced design where each module set contributes a portion of the total failure probability as nearly equal as possible to other contributors of failure probability. Thus, improving the highest failure probability device adds the most to system improvement. A variation of this technique is one where a calculation of the change in survivability per unit weight (or power) is made for each subsystem, and then the redundancy increase is made in the subsystem showing the largest quotient.

The elements that influence the system survivability prediction are the partitioning of the system and the parameters of the analytic model. The partitioning is a function of the system design and is difficult to change. Of the modeling parameters, mission time is fixed. Parts selection can improve failure rate, while improvements to fault tolerance methods can enhance the components of coverage.

The baseline Shuttle avionics system survivability for the ALT mission time is "driven" by the peripheral device detectabilities. Improvement of this parameter adds a marked improvement to the Shuttle survivability prediction. Increasing the detectability from .999 to .9999 gives four-fold improvements in failure probability. Further improvements add less. The system survivability is still dominated by the high failure rate forward flight critical bus devices. At a detectability of .9999, increasing the redundancy could help, but this doesn't seem feasible at this stage of development. An interesting point is that at a detectability of .999, the predicted failure rates and the ALT mission time, redundancy increases are counter-productive. For example, the IMU with a redundancy of 3 has a better survivability prediction at six hours than the ADTA with a smaller failure rate and a redundancy of 4. This is not true for a detectability of .9999 or for a mission time of 20 hours.

In the baseline parameter set, GPC recoverability was chosen to be 1. If switching off a faulty GPC is done manually by a human operator, then fault recovery time is governed by human reaction time, and the correctness of the

recovery action taken is degraded by a panic situation during time-critical phases. We know that if this degradation results in a GPC recoverability as small as .999, then it becomes a very important factor to be considered. If this is the case, other GPC options such as transient recovery become important. Perhaps a way of obtaining sufficient memory space and GPC operations rate to allow automatic switchout of a faulty GPC would be to commit more of the IOP operations to microprogram.

Automatic use of an alternate MDM port during time-critical phases is not useful. However, for orbital flight, the use of alternate ports for reconfiguration at the beginning of deorbit will enhance the probability of beginning descent at full redundancy.

6.5 SYSTEM MODEL VERIFICATION

The modeling presented here is thought to be a true representation of the Shuttle avionics system for ALT. Certain laboratory tests are possible to verify the model. Faults may be physically injected into the system, and the resulting recovery may be observed. Since the model presented here is probabilistic, the faults should be chosen at random according to the failure rate of the parts. The system fails if it is no longer capable of performing all its critical functions. Protective redundancy used by the system means that more than one fault may be sustained before the system fails. But a single uncovered fault may cause the system to fail.

The first approach is to generate faults for a series of six-hour missions, inject the faults, and record the results. The resulting failure probability is the number of failed missions divided by the total number of missions. This approach is straightforward but can't be done in a reasonable amount of time in practice. The reason is that system failures occur approximately once every 10,000 missions, on the average. One or more faults occur in about one out of ten missions, so that, on the average, 1000 missions would have to be experimentally checked for each system failure. About 200 system failures should occur for an approximate system model verification. The resulting 200,000 experiments are a formidable task.

A method to reduce the magnitude of this is to extend the mission time to where the probability of failure is much greater, say .1 or .2. This only tests a generally uninteresting extreme prediction.

Methods should be sought to reduce the size of the task. The number of experiments can be reduced by concentrating on a portion of the system. This eliminates the sizeable number of missions that have several faults, but only a single fault in each device.

Another method, which can be used in conjunction with the first, is to realize that the probability of <u>exactly</u> k faults occurring in a mission of length T on a system or portion of a system with <u>total</u> failure rate λ is is $P(k) = e^{-\lambda T} (\lambda T)^k / k!$. Experiments are then run 1, 2, 3, etc. faults to obtain failure statistics on the number of faults per mission. The resulting failure probability is then

$$F(T) = \sum_{k=1}^{n} P(k) \frac{\text{Number of failures with k faults}}{\text{Number of missions with k faults}}$$

The GPCs would be a desirable unit to apply this kind of experiment. With a coverage of 1 for the first two faulty GPCs, we can concentrate on missions with three or more faults. Evaluating P(k) for k = 3, 4, 5, λ = 4000/106 hours and T - 6 hours.

$$P(3) \approx e^{-.024} \frac{(.024)^3}{3!} = 2.3(10)^{-6}$$

$$P(4) \approx 1.8(10)^{-8}$$

$$P(5) \approx 6.6(10)^{-11}$$

Three fault missions have a large impact on the GPC failure probability of $3.5(10)^{-7}$; four fault missions, at most, affect the failure probability by ± 2 in second significant digit; and five fault missions have little impact on the failure probability prediction. Therefore, experimentation can be confined to three fault missions. We would expect about 5 to 10 percent of the three fault missions to fail. One thousand missions should result in 50 to 100 failures. Fault patterns where the three faults occur in at most 2 GPCs need not be performed, and may be counted as a non-failed mission. In performing the experiments, any failure after one or two faults indicates the GPC coverage is less than one.

The next question is how to inject the faults into the system. The first method is for a technician to physically open or short the electrical points chosen by random number generation, and record the results. This is a tedious job, but requires the least development of specialized equipment. A more elegant and rapid method would be to electrically inject the faults under minicomputer control. This has the added advantage that the random faults may be generated by the minicomputer. The disadvantage of this method is the development time and expense of this additional, specialized test equipment.

7.0 CONCLUSIONS AND RECOMMENDATIONS

7.1 CONCLUSIONS

Five significant conclusions were drawn from the work performed on the Shuttle avionics survivability analysis project. These are presented in prose in the following paragraphs, and summarized in Table 7.1-I on the facing page.

The accuracy of the prediction of the components of coverage for the various avionics subsystems is crucial with respect to the accuracy attainable in the overall survivability prediction. This is particularly true for units whose coverage components, e.g., detectability, are in the region of 0.999. For example, a change from 0.999 to 0.9999 lowers the safety-critical failure probability by a factor of four.

Use of the alternate MDM port for reconfiguration of GPC bus assignments will become useful when TACAN and/or microwave scan beam landing system units with lower failure rates become available.

The use of a recovery technique consisting of rollahead combined with memory copy has the potential of reducing transient leakage to zero (i.e., no transient faults are mistaken for permanents). This compares with the result of 70.3% when using the baseline technique of delay recovery. This more sophisticated GPC transient-fault recovery technique is most useful in hostile transient-fault environments, or when GPC coverage is degraded.

Improvement in TACAN detectability offers the most promise of improving the overall avionics failure probability. For example, improving the TACAN detectability from 0.999 to 0.9999, will decrease the overall avionics failure probability from $7.7(10)^{-5}$ to $5.6(10)^{-5}$.

Laboratory testing to verify the models presented here is feasible, but the testing must be carefully designed so as to obtain the maximum results in a reasonable test time. This test design includes both the test procedure and the test implementation, e.g., computer programs for automatic fault injection.

TABLE 7.1-I CONCLUSIONS

- Overall survivability accuracy depends critically on coverage-component accuracy
- Reconfiguration using the alternate MDM port is efficacious for lower failure rate units
- An alternative GPC recovery technique can reduce transient-fault leakage to zero
- Improving TACAN detectability offers the most promise for decrease of overall failure probability

7.2 RECOMMENDATIONS

The principal recommendation resulting from the performance of this study is that both the analytic model and simulator portion of CAST be further enhanced so that the OFT mission configuration can be modeled. This enhancement is required because of the ALT-OFT differences discussed below and summarized in Table 7.2-I.

The mission time-line of OFT consists of the ascent, orbit operations, and return portions, each of which is divided into more detailed phases. ALT encompasses only the late TAEM and approach and landing phases. These differences cause two aspects to need to be taken into account in the OFT modeling and simulation. First, it is necessary to adjust the planned DPS configuration as each new phase is entered. For example, during orbit two GPCs are operated in concert, while during return four GPCs are used. Second, it is necessary to model the fact that phases subsequent to the first may be entered with fewer than the planned complement of units operating. This results in probabilistic initial conditions for the second and later phases. It is thought that modeling work will be applicable here. In the simulator, this problem is approached by beginning each phase with the fault conditions encountered at the close of the previous phase.

The MCDS required a special model for ALT. The addition of an extra DEU for OFT will require new analytic and simulation models.

The GPC model applies to the ALT configuration of DDUs, but in OFT the additional DDU with only an ADI attached leads to a modeling situation similar to that encountered in the flight-critical MDMs. Thus, the flight-critical MDM model is applicable here. The addition of the EIU and MEC to the flight-critical bus leads to a change in the simulation of the flight-critical bus and additional models for these.

The remaining partitions can be modeled by the "standard" GPC model. However, there is an impact on the simulation. New programs are required from mass memory for changes in mission phase. Therefore, there is a strong interaction between MM and the GPC for OFT and this must be modeled. Also, the survival of the return phase programs becomes an important issue.

TABLE 7.2-I ALT-OFT DIFFERENCES

ANALYTIC MODEL

ITEM	ALT	OFT
Mission Time Line	Single Configuration Deterministic Initial Conditions	Several Configurations Probabalistic Initial Conditions For Each Phase
MCDS	Special Model	New Model Required
DDU, FFMDM, FAMDM	Special Model	Adaptation of Special Model
GPC, PCMMU, MM, PLDMDM	GPC Model Applies	GPC Model Applies
EIU, MEC, MCIU, SRBMDM	Not Used	GPC Model May Apply

SIMULATOR

ITEM	ALT	OFT
Mission Time Line	Only One Phase is Simulated	Several Phases - Each with Different Configurations. Initial Conditions for Each Phase Determined by Status of Previous Phase.
MCDS Partition	Simulated by Separate Subroutines	New Model Required
FCBUS Partition	Model Includes: DDU, FF-MDM, FA-MDM and Their Associated Devices	Need to Add Simulation Models for EIU's and MEC's
GPC Partition	Quadruplex Configuration SM Functions in Redundant Set	Configuration Varies Depending on Mission Phase SM Function Removed from Redundant Sett Software Reconfiguration from MM at Phase Changes
Mission Critical Devices MM, PCM	Not Used	Simulation Required

THIS PAGE INTENTIONALLY LEFT BLANK

REFERENCES

FREU 62 Freund, J., Mathematical Statistics, pp 232-233, Prentice-Hall, 1962.

HILL 70 Hillier, F.S., and Lieberman, G.J., Introduction to Operations Research, pp 447-450, Holden-Day, Inc., San Francisco, 1970.

KRUU 63 Kruus, J., "Upper Bounds for the Mean Life of Self-Repairing Systems," Report R-172 Coordinated Science Laboratory, University of Illinois, July 1963.

PARZ 60 Parzen, E., Modern Probability Theory and Its Applications, pp 251-263, Wiley & Sons, 1960.

SHRE 66 Shreider, Y.A., The Monte Carlo Method, Pergamon Press, New York, 1966.