

INDEPENDENT ORBITER ASSESSMENT

ANALYSIS OF THE BACKUP FLIGHT SYSTEM

8 DECEMBER 1986



MCDONNELL DOUGLAS ASTRONAUTICS COMPANY
HOUSTON DIVISION

SPACE TRANSPORTATION SYSTEM ENGINEERING AND OPERATIONS SUPPORT

WORKING PAPER NO. 1.0-WP-VA86001-18

INDEPENDENT ORBITER ASSESSMENT
ANALYSIS OF THE BACKUP FLIGHT SYSTEM

8 December 1986

This Working Paper is Submitted to NASA under
Task Order No. VA86001, Contract NAS 9-17650

PREPARED BY: E.E. Prust
E.E. Prust
Analyst
Independent Orbiter
Assessment

APPROVED BY: _____
J.J. Ewell, Jr.
BFS Lead
Independent Orbiter
Assessment

PREPARED BY: L.W. Hinsdale
L.W. Hinsdale
Analyst
Independent Orbiter
Assessment

APPROVED BY: G.W. Knori
G.W. Knori
Technical Manager
Independent Orbiter
Assessment

PREPARED BY: R.W. Mielke
R.W. Mielke
Analyst
Independent Orbiter
Assessment

APPROVED BY: W.F. Huning
W.F. Huning
Deputy Program Manager
STSEOS

CONTENTS

	Page
1.0 EXECUTIVE SUMMARY	1
2.0 INTRODUCTION	4
2.1 Purpose	4
2.2 Scope	4
2.3 Analysis Approach	4
2.4 BFS Ground Rules and Assumptions	5
3.0 SUBSYSTEM DESCRIPTION	6
3.1 Design and Function	6
3.2 Interfaces and Locations	10
3.3 Hierarchy	10
3.4 BFS Sensitivity to Interfacing Subsystem Operation	10
3.4.1 Inertial Measurement Unit (IMU)	11
3.4.2 Air Data System (ADS)	11
3.4.3 Rate Gyro Assemblies (RGA) and Accelerometer Assembly (AA)	11
3.4.4 Rotational Hand Controller (RHC)	12
3.4.5 Speedbrake Thrust Controller (SBTC)	12
3.4.6 Rudder Pedal Transducer Assembly (RPTA)	12
3.4.7 Cockpit Switches	12
4.0 ANALYSIS RESULTS	14
4.1 Dedicated Display Unit (DDU)	15
4.2 Backup Flight Controllers (BFC)	15
4.3 General Purpose Computer (GPC)	15
4.4 Switches (SW)	15
4.5 Circuit Protection (CP)	16
4.6 Indicators (IND)	16
5.0 REFERENCES	17
APPENDIX A ACRONYMS	A-1
APPENDIX B DEFINITIONS, GROUND RULES, AND ASSUMPTIONS	B-1
B.1 Definitions	B-2
B.2 Project Level Ground Rules and Assumptions	B-4
B.3 Subsystem Specific Ground Rules and Assumptions	B-6
APPENDIX C DETAILED ANALYSIS	C-1
APPENDIX D POTENTIAL CRITICAL ITEMS	D-1

List of Figures

	Page
Figure 1 - BFS OVERVIEW ANALYSIS SUMMARY	3
Figure 2 - BFS SUBSYSTEM OVERVIEW	7
Figure 3 - BFS ENGAGE/DISENGAGE HARDWARE AND DATA INTERFACES	8

List of Tables

	Page
Table I - SUMMARY OF IOA FAILURE MODES AND CRITICALITIES	14
Table II - SUMMARY OF IOA POTENTIAL CRITICAL ITEMS	14

Independent Orbiter Assessment
Analysis of the Backup Flight System

1.0 EXECUTIVE SUMMARY

The McDonnell Douglas Astronautics Company (MDAC) was selected in June 1986 to perform an Independent Orbiter Assessment (IOA) of the Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL). Direction was given by the STS Orbiter and GFE Projects Office to perform the hardware analysis using the instructions and ground rules defined in NSTS 22206, Instructions for Preparation of FMEA and CIL, 10 October 1986. The IOA approach features a top-down analysis of the hardware to determine failure modes, criticality, and potential critical items. To preserve independence, this analysis was accomplished without reliance upon the results contained within the NASA FMEA/CIL documentation. This report documents (Appendix C) the analysis results corresponding to the Orbiter Backup Flight System (BFS) hardware.

The BFS hardware consists of one General Purpose Computer (GPC) loaded with backup flight software and the components used to engage/disengage that unique GPC. Specifically, the BFS hardware includes the following:

- o DDU (Display Driver Unit)
- o BFC (Backup Flight Controller)
- o GPC (General Purpose Computer)
- o Switches (Engage, Disengage, GPC, CRT)
- o Circuit Protectors (Fuses, Circuit Breakers)

The IOA analysis process utilized available BFS hardware drawings and schematics for defining hardware assemblies, components, and hardware items. Each level of hardware was evaluated and analyzed for possible failure modes and effects. Criticality was assigned based upon the severity of the effect for each failure mode.

Figure 1 presents a summary of the failure criticalities for each of the major divisions of the BFS. A summary of the number of failure modes, by criticality, is also presented below with Hardware (HW) criticality first and Functional (F) criticality second.

Summary of IOA Failure Modes By Criticality (HW/F)							
Criticality:	1/1	2/1R	2/2	3/1R	3/2R	3/3	TOTAL
Number :	16	3	-	2	2	6	29

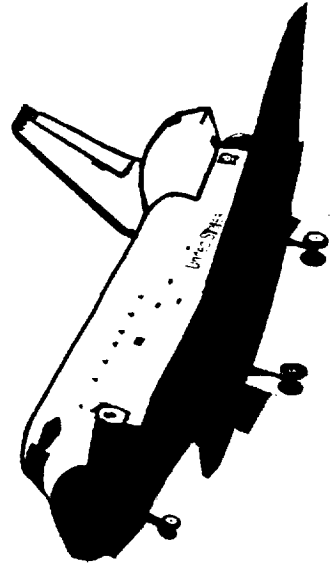
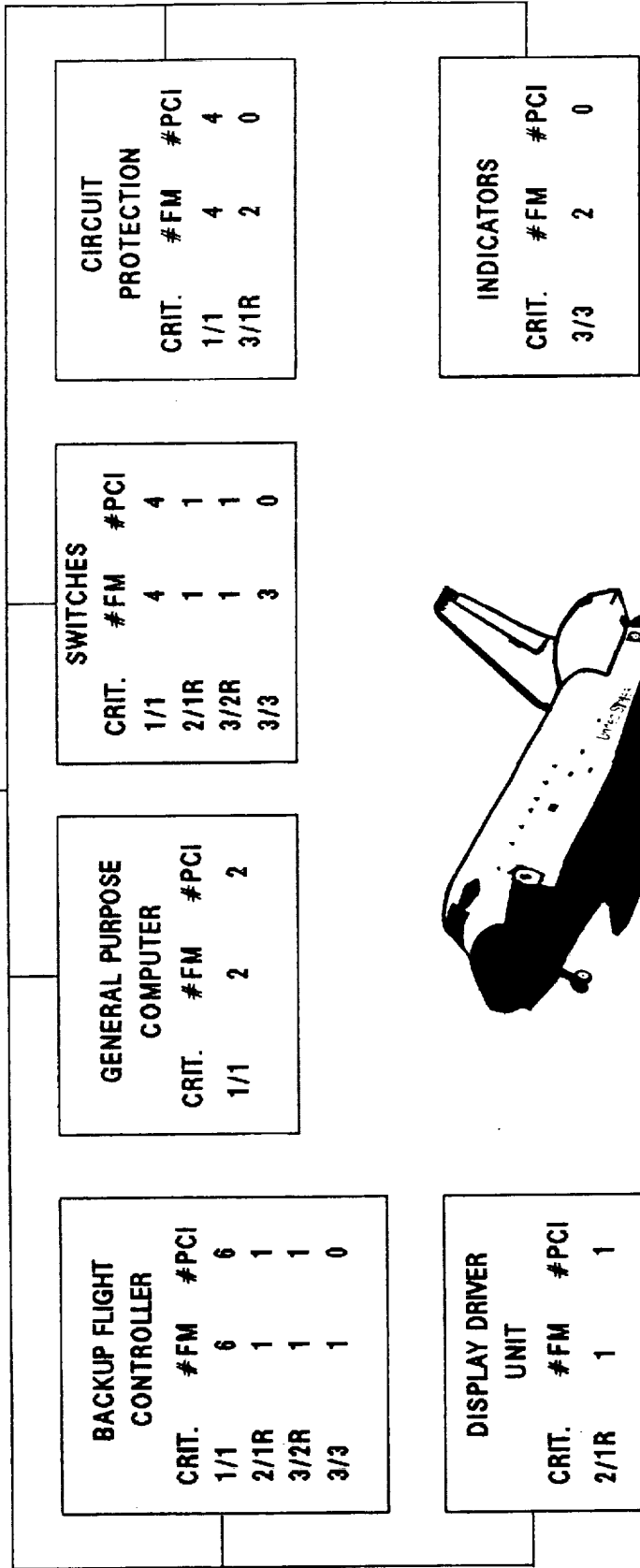
For each failure mode identified, the criticality and redundancy screens were examined to identify critical items. A summary of Potential Critical Items (PCIs) is presented as follows:

Summary of IOA Potential Critical Items (HW/F)						
Criticality:	1/1	2/1R	2/2	3/1R	3/2R	TOTAL
Number :	16	3	-	-	2	21

Of the failure modes analyzed, 19 could potentially result in a loss of life and/or loss of vehicle.

BFS OVERVIEW ANALYSIS SUMMARY

BFS ANALYSIS SUMMARY					
CRIT.	#FM	#PCI	CRIT.	#FM	#PCI
1/1	16	16	3/2R	2	2
2/1R	3	3	2/2	0	0
3/1R	2	0	3/3	6	0



CRIT - CRITICALITY
 FM - FAILURE MODE
 PCI - POTENTIAL CRITICAL ITEM

Figure 1 - BFS OVERVIEW ANALYSIS SUMMARY

2.0 INTRODUCTION

2.1 Purpose

The 51-L Challenger accident prompted the NASA to readdress safety policies, concepts, and rationale being used in the National Space Transportation System (NSTS). The NSTS Office has undertaken the task of reevaluating the FMEA/CIL for the Space Shuttle design. The MDAC is providing an independent assessment of the Orbiter FMEA/CIL reevaluation results for completeness and technical accuracy.

2.2 Scope

The scope of the independent FMEA/CIL assessment activity encompasses those Shuttle Orbiter subsystems and GFE hardware identified in the Space Shuttle Independent FMEA/CIL Assessment Contractor Statement of Work. Each subsystem analysis addresses hardware, functions, internal and external interfaces, and operational requirements for all mission phases.

2.3 Analysis Approach

The independent analysis approach is a top-down analysis utilizing as-built drawings to divide the respective subsystem into components and low-level hardware items. Each hardware item is evaluated for failure mode, effects, and criticality. These data are documented in the respective subsystem analysis report, and are used to assess the NASA and Prime Contractor FMEA/CIL reevaluation results. The IOA analysis approach is summarized in the following Steps 1.0 through 3.0. Step 4.0 summarizes the assessment of the NASA and Prime Contractor FMEAs/CILs that is performed and documented at a later date.

Step 1.0 Subsystem familiarization

- 1.1 Define subsystem functions
- 1.2 Define subsystem components
- 1.3 Define subsystem specific ground rules and assumptions

Step 2.0 Define subsystem analysis diagram

- 2.1 Define subsystem
- 2.2 Define major assemblies
- 2.3 Develop detailed subsystem representations

Step 3.0 Failure events definition

- 3.1 Construct matrix of failure modes
- 3.2 Document IOA analysis results

Step 4.0 Compare IOA analysis data to NASA FMEA/CIL

- 4.1 Resolve differences
- 4.2 Review in-house
- 4.3 Document assessment issues
- 4.4 Forward findings to Project Manager

2.4 BFS Ground Rules and Assumptions

The BFS specific ground rules and assumptions used in the IOA are presented in Appendix B.

3.0 SUBSYSTEM DESCRIPTION

The following sections describe the BFS hardware. This hardware comprises a GPC, DDU's, BFCs, several switches, status indicators, and circuit protectors. An overview of the system components is shown in Figure 2.

3.1 Design and Function

The Backup Flight System provides the flight crew with a vehicle control capability to be used if the primary system malfunctions. The BFS software resides in one GPC, normally GPC 5, during ascent and entry. In the event a generic failure occurs in the Primary Avionics Software System (PASS) or three or more primary GPCs fail, the crew will engage the BFS. During dynamic flight phases (e.g. not on-orbit) return to the primary system is not provided once the BFS is engaged.

Hardware elements included in this report are those specific to the BFS. Evaluation of specific components such as navigation aids, flight control sensors that are common to the BFS and the PASS, and components such as dedicated instrument displays that are driven by the BFS outputs are not included in this report. Processing schemes differ between PASS and BFS with the result that some component failures become more critical with BFS engaged. It is beyond the scope of this report to present all the software differences between PASS and BFS or to present a comparison of the failure criticalities for non-BFS-unique hardware with or without BFS engaged.

The BFS is limited by definition, for this report, to those unique hardware items that function in response to the action taken by the flight crew to engage or disengage the BFS. Reference Figure 3. More specifically, the BFS consists of the following components:

1. Two DDUs which supply power to the BFS engage switches on the left and right Rotation Hand Controllers (RHCs) and to the Hand Controller Engage Drivers (HCEDs) in the Backup Flight Controller (BFC) modules. Each DDU has three power supplies (A, B, and C) redundantly tied through regulators to two of the three Main A, B, and C buses.
2. Three BFCs, each with identical modules A and B, receive inputs from crew configured switches, and output discrete signals to their respective GPCs. Logic circuits select which GPCs control flight critical buses and drive CRT displays prior and subsequent to BFS engagement.
3. One GPC loaded with backup flight software. From a hardware standpoint, a GPC consists of a Central Processing Unit (CPU) and Input/Output Processor (IOP),

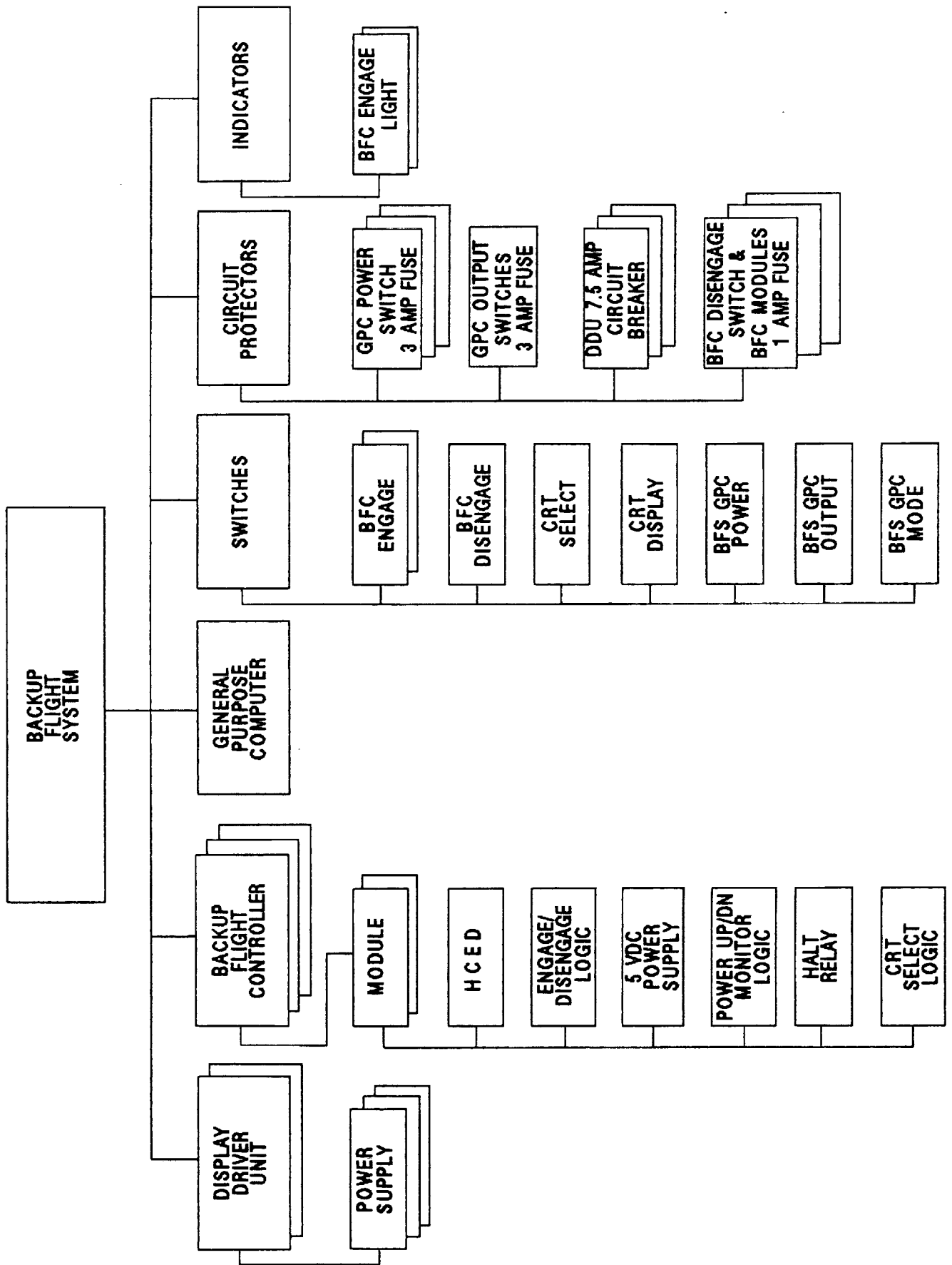


Figure 2 - BFS SUBSYSTEM OVERVIEW

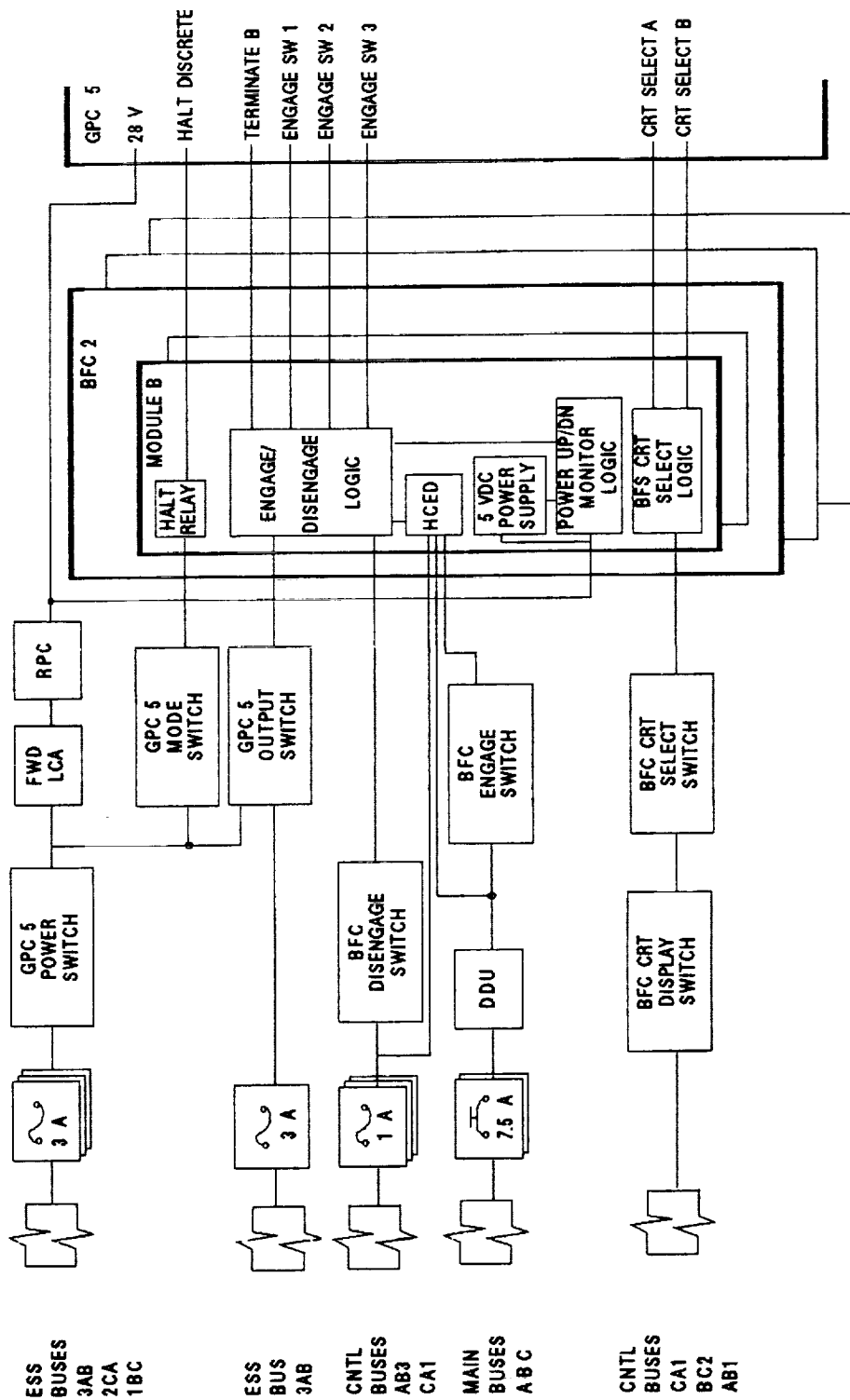


Figure 3 - BFS ENGAGE/DISENGAGE HARDWARE AND DATA INTERFACES

each with many subcomponents. Since there is only one GPC to provide the backup control capability, it will be treated as a black box. Regardless of what hardware-component failure renders the GPC inoperable, the criticality is the same as a generic black-box failure.

4. Twenty crew-activated switches (15 GPC, 2 BFS engage, 1 BFS disengage, and 2 CRT) are used to control the GPC operating configuration and CRT interfaces with the BFS GPC.
5. Crew interface with the BFS is through the Multifunction CRT Display System (MCDS). During normal flight operations, one of the Cathode Ray Tubes (CRTs) in the forward station will be commanded by the BFS. BFS MCDS selection in the forward station is governed by the BFS CRT switch on panel C3 or the GPC/CRT key on the keyboard. Current preengage BFS procedures call for CRT3 to be the BFS CRT in the forward station.

The BFS operates in one of two operating states: engaged and disengaged. The BFS is intended to remain in a disengaged state during routine operations allowing the PASS to control the vehicle. Both the engage and disengage states are provided to the GPCs through the BFCs. These BFCs provide interface through a series of discrete signals between the GPCs and associated crew-station switches. Engage is accomplished by verifying that the BFS GPC output switch is in the backup position, DDU power-supply breakers in, and depressing the engage-momentary pushbutton on either right or left RHC.

When one of the RHC pushbuttons is depressed, three discrettes (A, B, C) of ones are sent to the BFS GPC. The BFS GPC must receive two of three discrettes plus a zero discrete from the I/O terminate B before the BFS can be engaged. After the BFS is engaged, control of the vehicle is assumed by the BFS, and the PASS GPCs go to a state of software halt. The BFS then controls the flight-critical and payload-data buses and specified display-keyboard buses. Indications that the BFS is engaged are that BFC eyebrow panel lights on F2 and F4 will be ON, BFS output talkback (TB) on panel O6 will be gray, and all PASS GPCs output TBs on panel O6 will be barberpole.

In the disengaged state, the BFS GPC processes vehicle-control parameters in parallel with the PASS GPCs. During the disengage state, the BFS maintains knowledge of the vehicle state by listening on the flight-critical data buses commanded by the PASS GPCs. The disengaged BFS GPC also performs limited SM and FDA functions during OPS 1, 3, and 6. To disengage the BFS from the engage state, the BFC disengage switch on panel F6 is positioned to DISENGAGE (up position). The engage discrettes to the BFS will be reset to zero and the I/O terminate discrete set to one. Control of the FC and PL data buses will be released to the PASS. This is indicated by the BFC light going OFF, the PASS output TBs

going gray, and BFS output TB going barberpole. The PASS GPCs must be re-Initial Program Loaded (re-IPLed) prior to disengage. Thus the BFS disengage capability is provided only during quiescent vehicle flight.

If BFS is engaged it will drive several dedicated instrument displays in the forward station. This is instrumentation needed to safely fly the vehicle during the final phases of entry and landing. Two of the three Altitude Director Indicators (ADIs) are driven by the BFS in OPS 1 and OPS 3. The four scales (Alpha, Accel, M/Vel, EAS) of the Alpha/Mach Indicator (AMI) are driven by BFS in OPS major modes 304 and 305. Likewise, the four scales (Alt Accel, Alt Rate, Alt, Rad Alt) of the Altitude/Vertical Velocity Indicator (AVVI) are driven by engaged BFS in major modes 304 and 305. The Horizontal Situation Indicator (HSI) provides magnetic heading, course, course deviation, glide-slope deviation, and primary and secondary bearing, and the Surface Position Indicator (SPI), provides elevons, body flap percent, rudder, aileron, and speedbrake percent. The HSI and SPI are driven by the engaged BFS.

3.2 Interfaces and Locations

The BFS GPC and three BFCs are located in Avionics Bays 1 and 2. All other hardware components are located in the forward flight deck. The BFS interfaces with Orbiter subsystems via the flight-critical and payload data buses and flight-forward and flight-aft MDMS.

3.3 Hierarchy

Figure 2 illustrates the hierarchy of the BFS hardware components.

3.4 BFS Sensitivity to Interfacing Subsystem Operation

An exhaustive comparison of the BFS and PASS is beyond the scope of this report. However, a limited investigation of BFS sensitivity to operation in certain guidance, navigation, and control subsystems was performed. References 12 and 13 constituted the BFS capability description for this investigation.

Compared to the PASS the BFS capability for fault detection is minimal due to minimum redundancy management capability. As a result the BFS is substantially more vulnerable to malfunctions in interfacing subsystems. The specific subsystems investigated included the Inertial Measurement Units (IMUs), Air Data System (ADS), Rate Gyro Assemblies (RGA) and Accelerometer Assemblies (AA), Rotational Hand Controller (RHC), Speedbrake Thrust Controller (SBTC), Rudder Pedal Transducer Assembly (RPTA), and a limited collection of cockpit switches.

3.4.1 Inertial Measurement Unit (IMU)

The BFS does not use the Built in Test Equipment (BITE) or the ECHO features provided by IMU hardware. The BFS only faults an IMU when it has detected a Communications Fault (COM FAULT). In nominal operations the BFS uses a mid-value select. If an IMU is COM FAULTED, the lowest numbered IMU which has not been COM FAULTED will be selected. If two IMUs have been COM FAULTED, then data from the remaining IMU will be processed. If all three IMUs are COM FAULTED, the system will then try to reselect the last failed IMU.

This data-selection process makes the BFS extremely sensitive and vulnerable to IMU number 1 malfunctions which do not result in a COM FAULT on IMU number 1. Without regard to IMU number 1 performance, a simple COM FAULT on either IMU number 2 or 3 will allow that performance to be immediately propagated throughout the entire GN&C system.

3.4.2 Air Data System (ADS)

The data from this subsystem is vital to many computations, since several of the items measured by this subsystem are used throughout the GN&C software. The main item of concern is the Nose Landing Gear Uplock Discrete, V51X0300X. This discrete is used by the BFS software to determine if a correction factor is applied in the angle-of-attack calculation, the corrected static-pressure calculation, and the corrected total-pressure calculation. These three terms are then used to determine Mach Number, Pressure Altitude, Dynamic Pressure (Q -Bar), Equivalent Airspeed (EAS), and Estimated True Airspeed. The inclusion of the correction factor in the calculation is due to changes in the flow around the ADS when the nose gear is down.

Depending on the size of the correction factor being applied, the corrected static-pressure and corrected total-pressure values could be changed to a significant degree. Any calculations which use these values in either a first order or second order calculation would be in error, and this error would be factored into the Guidance and Navigation functions. The errors could be large enough to cause a loss of the vehicle.

3.4.3 Rate Gyro Assemblies (RGA) and Accelerometer Assembly (AA)

The BFS uses only three of the four RGAs on the Orbiter and the Solid Rocket Boosters (SRB). The fourth RGA is not used. Similarly, the BFS uses only three of the

four AAs. Only one scale factor and bias is used for three Orbiter RGAs, and one scale factor and bias is used for the SRBs RGAs. Only one scale factor and bias is used for all AAs. The PASS provides scale factor and bias for each of the RGA and AA.

The use of a single set of scale factor and bias for a group of RGAs and AAs is acceptable if the LRUs are very consistent. If, however, the performance is not very consistent, the data coming back from the LRUs could have large over-compensated variations.

3.4.4 Rotational Hand Controller (RHC)

The BFS does not support RHC processing in ascent modes. The BFS does not validate the RHC inputs by using the data-good indicator as in the PASS. There is no requirement to process the left RHC data before or after the right RHC data. The lack of a requirement for the order of processing RHC data is different than that found in the PASS. There may be a need to process the Commander's inputs before the Pilot's, as is done in the PASS.

3.4.5 Speedbrake Thrust Controller (SBTC)

The BFS does not have manual-throttling capability in ascent as does the primary. The BFS does process both SBTC.

3.4.6 Rudder Pedal Transducer Assembly (RPTA)

The BFS processes only the Commander's inputs. There is no redundancy when the BFS is engaged.

3.4.7 Cockpit Switches

The following switches have redundant partners, one set at the Commander's station and another set at the Pilot's station. The BFS processes only those switches at the Commander's station. Pilot's station switches are not processed.

TACAN source for HSI	F6	S4	V72K8587X
MSBLS source for HSI	F6	S4	V72K8589X
NAV source for HSI	F6	S4	V72K8588X
ADI Attitude Ref PB a	F6	S3	V72K2051X
PB b			V72K2052X
ADI Attitude Inertial	F6	S3	V72K2015X
ADI Attitude LV/LH	F6	S3	V72K2016X
ADI Attitude reference	F6	S3	V72K2017X

There may be physically duplicated switches in the cockpit. However, since the BFS does not process some of them, the Pilot station switches can not be considered redundant to the Commander's switches.

4.0 ANALYSIS RESULTS

Detailed analysis results for each of the identified failure modes are presented in Appendix C. Table I presents a summary of the failure criticalities. Further discussion of each of these subdivisions and the applicable failure modes is provided in subsequent paragraphs.

TABLE I Summary of IOA Failure Modes and Criticalities							
Criticality:	1/1	2/1R	2/2	3/1R	3/2R	3/3	TOTAL
DDU	-	1	-	-	-	-	1
BFC	6	1	-	-	1	1	9
GPC	2	-	-	-	-	-	2
SW	4	1	-	-	1	3	9
CP	4	-	-	2	-	-	6
IND	-	-	-	-	-	2	2
TOTAL	16	3	-	2	2	6	29

Of the 29 failure modes analyzed, 16 single failures were determined to result in loss of the crew or vehicle. A summary of the Potential Critical Items (PCIs) is presented in Table II. Appendix D presents a cross reference between each PCI and a specific worksheet in Appendix C.

TABLE II Summary of IOA Potential Critical Items						
Criticality:	1/1	2/1R	2/2	3/1R	3/2R	TOTAL
DDU	-	1	-	-	-	1
BFC	6	1	-	-	1	8
GPC	2	-	-	-	-	2
SW	4	1	-	-	1	6
CP	4	-	-	-	-	4
IND	-	-	-	-	-	-
TOTAL	16	3	-	-	2	21

4.1 Display Driver Unit (DDU)

The analysis of the DDU examined one failure mode for the three power supplies. The DDU powers the HCEs and the BFS engage pushbutton. Loss of power from two or more power supplies may disable BFS engage capability. If the BFS is needed, this could result in loss of the crew and vehicle. This failure has been identified as a PCI and is listed in Appendix D.

4.2 Backup Flight Controller (BFC)

The BFC analysis considered nine failure modes for six components. Of these, eight PCIs were identified and are listed in Appendix D.

The BFC implements the BFS engage and disengage commands. In addition, it houses the BFS CRT-select logic and the halt relay to the interfacing GPC. Failure of the HCE, engage/disengage logic, BFC power supply or power up/down monitor logic, impairs the capability to engage the BFS. These components are therefore vital to the safety of the crew and vehicle.

Activation of a halt relay temporarily or permanently disables the interfacing GPC. Inadvertent operation of a halt relay can be catastrophic if it occurs in the BFC interfacing with the BFS GPC. Failure of the halt relay to operate when desired will, at worst, impact mission objectives.

The CRT-select logic performs a nonessential function, and its failure therefore has no serious consequences.

4.3 General Purpose Computer (GPC)

The GPC assigned to host BFS software was analyzed for two failure modes - loss of output and erroneous output. In either case, failure is catastrophic if the BFS is needed. Both failures have been identified as PCIs and are listed in Appendix D.

4.4 Switches (SW)

The switch analysis considered nine failure modes for seven switches. Six of the nine failure modes were identified as PCIs and are listed in Appendix D.

Switches that are vital to proper engage and operation of the BFS include the engage pushbuttons, the disengage switch and the BFS GPC power, output, and mode switches. Failure of these switches may endanger the crew and vehicle.

The CRT display and select switches are nonessential. The worst-case effect of a failure of one of these two switches is a minor change in crew procedure.

4.5 Circuit Protection (CP)

The circuit protection analysis examined the "open circuit" failure for six circuit protectors. Power to discretes and hardware components is vital to the operation of BFS hardware; therefore, failure of any circuit protector has a potential safety impact to the crew and vehicle. Four of the six failure modes were identified as PCIs and are listed in Appendix D.

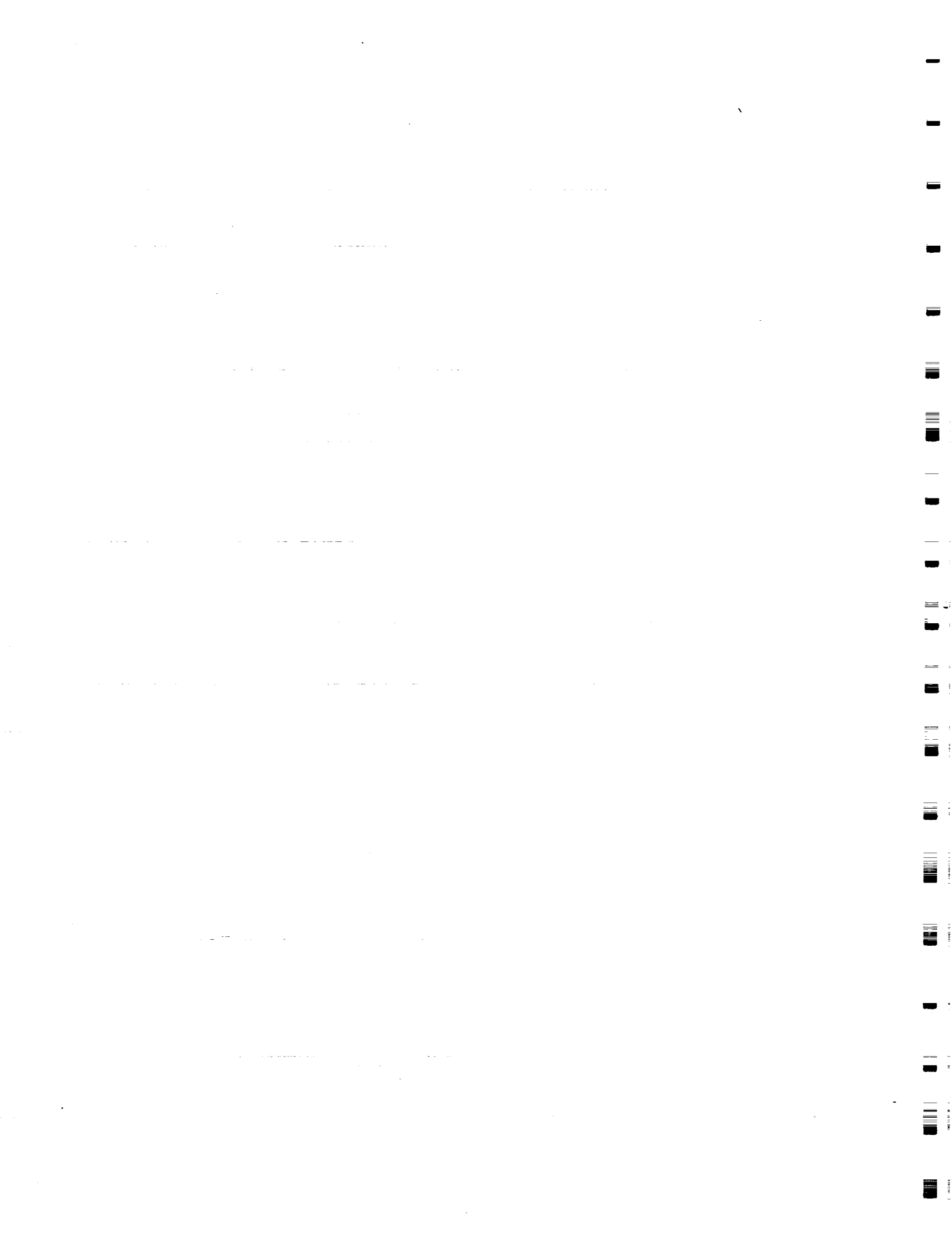
4.6 Indicators (IND)

The BFC engage light is the one indicator unique to the BFS. Two failure modes were analyzed and no PCIs were identified. Other indicators are available to show BFS engage/disengage status and operational status for all GPCs.

5.0 REFERENCES

Reference documentation available from NASA and Rockwell was used in the analysis. The documentation used included the following:

1. NSTS 22206: Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL), 10 October 1986
2. JSC 18820: Data Processing System Briefs, Basic, Rev. A, PCN-1, 4-20-85
3. VS70-971099: Rockwell Integrated Systems Schematics, OV-099, 103, 104 GNC & DPS, 3-14-85
4. JSC 12770: Shuttle Flight Operations Manual, Volume 5, Data Processing System, 3-21-84
5. JSC 18219: Flight Procedures Handbook, Post Insertion, Final Revision A, 1-18-85
6. JSC 18817: Flight Procedures Handbook, Deorbit Prep, 3-1-83
7. TD123: Backup Flight System Software Workbook, BFS 2102, 8-10-82
8. V72 FILE III: Orbiter Operations and Maintenance Requirements and Specification Document, 6-13-86
9. NSTS 08171 FILE I: Operations and Maintenance Requirements and Specifications Document, 7-14-86
10. JSC 12820: STS Operational Flight Rules, PCN-1, 2-14-86
11. TD198/A198: GNC Overview Workbook, GNC OV 2102, 8-30-83
12. MG038101: Backup System Service Program, Requirement Document, Seq. 1, Rev. H, 3 January 1985
13. MG038106: Backup Flight System, Hardware Interface Program and GN&C Interface Program Requirements Document, Rev. E, 3 July 1985



APPENDIX A
ACRONYMS

ADTA	-	Air Data Transducer Assembly
AOA	-	Abort Once Around
ATO	-	Abort to Orbit
BFC	-	Backup Flight Controller
BFS	-	Backup Flight System
BSS	-	Backup System Services
CIL	-	Critical Items List
CPU	-	Central Processing Unit
CRIT	-	Criticality
CRT	-	Cathode Ray Tube
C&W	-	Caution and Warning System
DDU	-	Display Driver Unit
DEU	-	Display Electronics Unit
DPS	-	Data Processing System
DU	-	Display Unit
EVA	-	Extra Vehicular Activity
FA	-	Flight Aft
FF	-	Flight Forward
FM	-	Failure Mode
FMEA	-	Failure Mode and Effects Analysis
GPC	-	General Purpose Computer
GSE	-	Ground Support Equipment
HCED	-	Hand Controller Engage Driver
IMU	-	Inertial Measurement Unit
IOA	-	Independent Orbiter Assessment
IOP	-	Input/Output Processor
IPL	-	Initial Program Load
KU	-	Keyboard Unit
LRU	-	Line Replaceable Unit
MCDS	-	Multifunction CRT Display System
MDAC	-	McDonnell Douglas Astronautics Company
MDM	-	Multiplexer/Demultiplexer
MM	-	Major Mode
MMU	-	Mass Memory Unit
NA	-	Not Applicable
NASA	-	National Aeronautics and Space Administration
NSTS	-	National Space Transportation System
OMRSD	-	Operational Maintenance Requirements and Specifications Document
OMS	-	Orbital Maneuvering System
PAS	-	Primary Avionics System
PASS	-	Primary Avionics Software System
PB	-	Pushbutton
PCI	-	Potential Critical Item
RCS	-	Reaction Control System
RHC	-	Rotational Hand Controller
RI	-	Rockwell International
RM	-	Redundancy Management
RPC	-	Remote Power Controller

RS - Redundant Set
RTLS - Return to Landing Site
SFP - Single Failure Point
SM - Systems Management
STS - Space Transportation System
SW - Software
Switch
TAC - Tacan
TAL - Transatlantic Abort Landing
TD - Touch Down
THC - Translational Hand Controller

APPENDIX B

DEFINITIONS, GROUND RULES, AND ASSUMPTIONS

- B.1 Definitions
- B.2 Project Level Ground Rules and Assumptions
- B.3 Subsystem-Specific Ground Rules and Assumptions

APPENDIX B
DEFINITIONS, GROUND RULES, AND ASSUMPTIONS

B.1 Definitions

Definitions contained in NSTS 22206, Instructions For Preparation of FMEA/CIL, 10 October 1986, were used with the following amplifications and additions.

INTACT ABORT DEFINITIONS:

RTLS - begins at transition to OPS 6 and ends at transition to OPS 9, post-flight

TAL - begins at declaration of the abort and ends at transition to OPS 9, post-flight

AOA - begins at declaration of the abort and ends at transition to OPS 9, post-flight

ATO - begins at declaration of the abort and ends at transition to OPS 9, post-flight

CREDIBLE (CAUSE) - an event that can be predicted or expected in anticipated operational environmental conditions. Excludes an event where multiple failures must first occur to result in environmental extremes

CONTINGENCY CREW PROCEDURES - procedures that are utilized beyond the standard malfunction procedures, pocket checklists, and cue cards

EARLY MISSION TERMINATION - termination of onorbit phase prior to planned end of mission

EFFECTS/RATIONALE - description of the case which generated the highest criticality

HIGHEST CRITICALITY - the highest functional criticality determined in the phase-by-phase analysis

MAJOR MODE (MM) - major sub-mode of software operational sequence (OPS)

MC - Memory Configuration of Primary Avionics Software System (PASS)

MISSION - assigned performance of a specific Orbiter flight with payload/objective accomplishments including orbit phasing and altitude (excludes secondary payloads such as GAS cans, middeck P/L, etc.)

MULTIPLE ORDER FAILURE - describes the failure due to a single cause or event of all units which perform a necessary (critical) function

OFF-NOMINAL CREW PROCEDURES - procedures that are utilized beyond the standard malfunction procedures, pocket checklists, and cue cards

OPS - software operational sequence

PRIMARY MISSION OBJECTIVES - worst case primary mission objectives are equal to mission objectives

PHASE DEFINITIONS:

PRELAUNCH PHASE - begins at launch count-down Orbiter power-up and ends at moding to OPS Major Mode 102 (liftoff)

LIFTOFF MISSION PHASE - begins at SRB ignition (MM 102) and ends at transition out of OPS 1 (Synonymous with ASCENT)

ONORBIT PHASE - begins at transition to OPS 2 or OPS 8 and ends at transition out of OPS 2 or OPS 8

DEORBIT PHASE - begins at transition to OPS Major Mode 301 and ends at first main landing gear touchdown

LANDING/SAFING PHASE - begins at first main gear touchdown and ends with the completion of post-landing safing operations

APPENDIX B
DEFINITIONS, GROUND RULES, AND ASSUMPTIONS

B.2 IOA Project Level Ground Rules and Assumptions

The philosophy embodied in NSTS 22206, Instructions for Preparation of FMEA/CIL, 10 October 1986, was employed with the following amplifications and additions.

1. The operational flight software is an accurate implementation of the Flight System Software Requirements (FSSRs).

RATIONALE: Software verification is out-of-scope of this task.

2. After liftoff, any parameter which is monitored by system management (SM) or which drives any part of the Caution and Warning System (C&W) will support passage of Redundancy Screen B for its corresponding hardware item.

RATIONALE: Analysis of on-board parameter availability and/or the actual monitoring by the crew is beyond the scope of this task.

3. Any data employed with flight software is assumed to be functional for the specific vehicle and specific mission being flown.

RATIONALE: Mission data verification is out-of-scope of this task.

4. All hardware (including firmware) is manufactured and assembled to the design specifications/drawings.

RATIONALE: Acceptance and verification testing is designed to detect and identify problems before the item is approved for use.

5. All Flight Data File crew procedures will be assumed performed as written, and will not include human error in their performance.

RATIONALE: Failures caused by human operational error are out-of-scope of this task.

6. All hardware analyses will, as a minimum, be performed at the level of analysis existent within NASA/Prime Contractor Orbiter FMEA/CILs, and will be permitted to go to greater hardware detail levels but not lesser.

RATIONALE: Comparison of IOA analysis results with other analyses requires that both analyses be performed to a comparable level of detail.

7. Verification that a telemetry parameter is actually monitored during AOS by ground-based personnel is not required.

RATIONALE: Analysis of mission-dependent telemetry availability and/or the actual monitoring of applicable data by ground-based personnel is beyond the scope of this task.

8. The determination of criticalities per phase is based on the worst case effect of a failure for the phase being analyzed. The failure can occur in the phase being analyzed or in any previous phase, whichever produces the worst case effects for the phase of interest.

RATIONALE: Assigning phase criticalities ensures a thorough and complete analysis.

9. Analysis of wire harnesses, cables, and electrical connectors to determine if FMEAs are warranted will not be performed nor FMEAs assessed.

RATIONALE: Analysis was substantially complete prior to NSTS 22206 ground rule redirection.

10. Analysis of welds or brazed joints that cannot be inspected will not be performed nor FMEAs assessed.

RATIONALE: Analysis was substantially complete prior to NSTS 22206 ground rule redirection.

11. Emergency system or hardware will include burst discs and will exclude the EMU Secondary Oxygen Pack (SOP), pressure relief valves and the landing gear pyrotechnics.

RATIONALE: Clarify definition of emergency systems to ensure consistency throughout IOA project.

APPENDIX B
DEFINITIONS, GROUND RULES, AND ASSUMPTIONS

B.3 BFS-Specific Ground Rules and Assumptions

1. BFS failures are analyzed assuming that the BFS is (or will be) engaged.

RATIONALE: Failure analysis and criticality determination is done assuming that the BFS must work when called upon to do so.

2. Failures which resulted in BFS engagement are not identified or analyzed.

RATIONALE: Except for the PASS, it is assumed that other subsystems are operating within normal limits.

3. Only BFS-specific components and failure modes are analyzed.

RATIONALE: Failure analysis of PASS/BFS common components is accomplished within the PASS analysis.

APPENDIX C
DETAILED ANALYSIS

This section contains the IOA analysis worksheets generated during the analysis of this subsystem. The information on these worksheets is intentionally similar to the NASA FMEAs. Each of these sheets identifies the hardware item being analyzed, and parent assembly, as well as the function. For each failure mode, the possible causes are outlined, and the assessed hardware and functional criticality for each mission phase is listed, as described in the NSTS 22206, Instructions for Preparation of FMEA and CIL, 10 October 1986. Finally, effects are entered at the bottom of each sheet, and the worst case criticality is entered at the top.

LEGEND FOR IOA ANALYSIS WORKSHEETS

Hardware Criticalities:

- 1 = Loss of life or vehicle
- 2 = Loss of mission or next failure of any redundant item (like or unlike) could cause loss of life/vehicle
- 3 = All others

Functional Criticalities:

- 1R = Redundant hardware items (like or unlike) all of which, if failed, could cause loss of life or vehicle.
- 2R = Redundant hardware items (like or unlike) all of which, if failed, could cause loss of mission.

Redundancy Screen A:

- 1 = Is Checked Out PreFlight
- 2 = Is Capable of Check Out PreFlight
- 3 = Not Capable of Check Out PreFlight
- NA = Not Applicable

Redundancy Screens B and C:

- P = Passed Screen
- F = Failed Screen
- NA = Not Applicable

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 2/1R
MDAC ID: 101 ABORT: 2/1R

ITEM: POWER SUPPLY A(B,C) TO L(R) RHC
FAILURE MODE: LOSS OF OUTPUT, PARTIAL OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) L, R DISPLAY DRIVER UNIT
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	2/1R
LIFTOFF:	2/1R	TAL:	2/1R
ONORBIT:	2/NA	AOA:	2/1R
DEORBIT:	2/1R	ATO:	2/1R
LANDING/SAFING:	2/1R		

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 33V73A1, 33V73A2
PART NUMBER: MC409-0023-0003 (DISPLAY DRIVER UNIT)

CAUSES: VIBRATION, CONTAMINATION, THERMAL STRESS, MECHANICAL SHOCK, PIECE PART STRUCTURAL FAILURE

EFFECTS/RATIONALE:

LOSS OF ONE POWER SUPPLY RESULTS IN LOSS OF CAPABILITY TO ENGAGE BFS USING ONE ROTATION HAND CONTROLLER (RHC).
A SECOND FAILURE, IF IT OCCURS IN A POWER SUPPLY TO THE REMAINING RHC, WILL RESULT IN TOTAL LOSS OF BFS ENGAGE CAPABILITY. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 201 ABORT: 1/1

ITEM: HALT RELAY
FAILURE MODE: INADVERTENT OPERATION, FAILS TO REMAIN OPEN

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	2/2	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [P] C [NA]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, ERRONEOUS INPUT

EFFECTS/RATIONALE:

INADVERTENT OPERATION OF A HALT RELAY STOPS THE PROCESSING OF
SOFTWARE IN THE INTERFACING GPC. A FAILURE OCCURING IN THE HALT
RELAY TO THE BFS GPC RENDERS THE BFS TEMPORARILY USELESS. LOSS
OF THE CREW/VEHICLE MAY RESULT.
FAILURE(S) OCCURING IN THE HALT RELAY(S) TO THE PASS GPC(S) ON-
ORBIT MAY IMPACT THE MISSION. A FAILURE OCCURING PRELAUNCH WILL
CAUSE A LAUNCH DELAY OR SCRUB.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/2R
MDAC ID: 202 ABORT: 3/3

ITEM: HALT RELAY
FAILURE MODE: FAILS TO CLOSE

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/2R	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [1] B [F] C [P]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, LOSS OF INPUT

EFFECTS/RATIONALE:

LOSS OF THE HALT RELAY TO A PASS GPC PREVENTS IPL OF THAT GPC.
THE GPC ALSO CANNOT BE POWERED OFF AND THEN BACK ON AGAIN.
MULTIPLE FAILURES MAY IMPACT THE MISSION.
LOSS OF THE HALT RELAY TO THE BFS GPC HAS NO IMPACT. BFS HAS
POWER-ON RESTART CAPABILITY; THEREFORE IT CAN BE POWERED ON AND
OFF WITHOUT BEING PUT INTO HALT.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 2/1R
MDAC ID: 203 ABORT: 2/1R

ITEM: HAND CONTROLLER ENGAGE DRIVER
FAILURE MODE: LOSS OF DISCRETE OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

	CRITICALITIES		
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	2/1R
LIFTOFF:	2/1R	TAL:	2/1R
ONORBIT:	3/NA	AOA:	2/1R
DEORBIT:	2/1R	ATO:	2/1R
LANDING/SAFING:	2/1R		

REDUNDANCY SCREENS: A [1] B [F] C [P]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

FAILURE OF ONE HCED CAUSES LOSS OF ENGAGE CAPABILITY FROM ONE
RHC. THE BROADCASTING OF AN ENGAGE DISCRETE TO THE BFC MODULES
IS DISABLED.

A SECOND FAILURE, IF IT OCCURS IN AN HCED INTERFACING WITH THE
REMAINING RHC, WILL RESULT IN TOTAL LOSS OF BFS ENGAGE
CAPABILITY. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 204 ABORT: 1/1

ITEM: HAND CONTROLLER ENGAGE DRIVER
FAILURE MODE: LOSS OF 28 VDC OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

THE HCED 28 VDC OUTPUT PROVIDES POWER TO THE ENGAGE LOGIC OPTICAL ISOLATORS. LOSS OF THIS POWER PREVENTS THE ENGAGE DISCRETES FROM BEING TRANSMITTED TO THE ENGAGE LOGIC. THE INTERFACING GPC WILL NOT RESPOND PROPERLY WHEN BFS ENGAGE IS ATTEMPTED. IF THIS FAILURE OCCURS IN THE BFC MODULE INTERFACING WITH THE BFS GPC (NORMALLY GPC 5), ENGAGE CAPABILITY IS LOST. LOSS OF THE CREW/VEHICLE MAY RESULT.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 205 ABORT: 1/1

ITEM: ENGAGE / DISENGAGE LOGIC
FAILURE MODE: LOSS OF OUTPUT, ERRONEOUS OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

INCORRECT OUTPUT FROM THE ENGAGE/DISENGAGE LOGIC INHIBITS THE
INTERFACING GPC FROM ENGAGING/DISENGAGING PROPERLY. THIS MAY
CAUSE LOSS OF THE CREW/VEHICLE DURING DYNAMIC FLIGHT PHASES.
THIS IS A SINGLE POINT FAILURE IF IT OCCURS IN THE BFC MODULE
INTERFACING WITH THE BFS GPC (NORMALLY GPC 5).

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 206 ABORT: 3/3

ITEM: CRT SELECT LOGIC
FAILURE MODE: LOSS OF OUTPUT, ERRONEOUS OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/NA	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [2] B [P] C [P]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

FAILURE OF THE BFC CRT SELECT LOGIC PREVENTS THE CORRECT BFS CRT
ASSIGNMENT FROM BEING BROADCAST TO THE INTERFACING GPC. BFS CRT
SELECTION MAY BE ACCOMPLISHED BY KEYBOARD ENTRY AS A BACKUP.
LOSS OF ALL MEANS OF ASSIGNING A CRT TO THE BFS CAUSES LOSS OF
BFS CRT DISPLAYS PRE-ENGAGE. POST-ENGAGE, BFS WILL CONTROL CRT'S
1 & 2 BY DEFAULT. SAFETY OF THE CREW/VEHICLE IF UNAFFECTED. IF
THE FAILURE OCCURS PRELAUNCH, LAUNCH MAY BE SCRUBBED.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 207 ABORT: 1/1

ITEM: BFC POWER SUPPLY (5 VDC)
FAILURE MODE: LOSS OF OUTPUT, PARTIAL OUTPUT, FAILS OUT OF TOLERANCE

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/2R	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

A FAILURE OF THE BFC POWER SUPPLY WILL INITIATE A RESET OF THE ENGAGE LATCHES BY THE POWER UP/DOWN MONITOR LOGIC. IF THIS OCCURS POST-ENGAGE IN THE BFC MODULE INTERFACING WITH THE BFS GPC, THE BFS WILL DISENGAGE. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

IN ADDITION, LOSS OF POWER TO THE GPC RUN/STANDBY/HALT DISCRETES WILL LEAVE THE GPC "STUCK" IN THE LAST VALID STATE. MULTIPLE FAILURES WILL PROBABLY IMPACT THE MISSION.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 208 ABORT: 1/1

ITEM: POWER UP/DOWN MONITOR LOGIC
FAILURE MODE: INADVERTENT OPERATION

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

INADVERTENT OPERATION OF THE POWER UP/DOWN MONITOR LOGIC WILL
RESET THE BFS ENGAGE DISCRETES. IF THIS OCCURS POST-ENGAGE IN
THE BFS MODULE INTERFACING WITH THE BFS GPC, THE BFS WILL
DISENGAGE.
THE BFS MAY BE RE-ENGAGED, BUT LOSS OF THE CREW/VEHICLE IS A
POSSIBILITY.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 209 ABORT: 1/1

ITEM: POWER UP/DOWN MONITOR LOGIC
FAILURE MODE: LOSS OF OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) BACKUP FLIGHT CONTROLLER
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 81V72A321, 81V72A322, 81V72A323; AVIONICS BAYS 1&2
PART NUMBER: MC615-0023 (BACKUP FLIGHT CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, CONTAMINATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

FAILURE OF THE POWER UP/DOWN MONITOR LOGIC TO DETECT POWER
OVERFLOW/UNDERFLOW MAKES CORRECT OPERATION OF THE
ENGAGE/DISENGAGE LOGIC QUESTIONABLE. IF THE FAILURE OCCURS IN
THE BFC MODULE INTERFACING WITH THE BFS GPC, ENGAGE/DISENGAGE MAY
BE INHIBITED.
THE WORST CASE EFFECT IS LOSS OF THE CREW/VEHICLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 301 ABORT: 1/1

ITEM: BACKUP GPC (USUALLY GPC 5)
FAILURE MODE: LOSS OF OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) GENERAL PURPOSE COMPUTER (GPC)
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [F]

LOCATION: AVIONICS BAY
PART NUMBER: IBM AP-101 CPU / IBM 4P1 IOP

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LOSS OF OUTPUT FROM THE BFS GPC WILL CAUSE LOSS OF VEHICLE
CONTROL WHEN THE BFS IS ENGAGED. LOSS OF THE CREW/VEHICLE IS
PROBABLE.

REFERENCES: JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 302 ABORT: 1/1

ITEM: BACKUP GPC (USUALLY GPC 5)
FAILURE MODE: ERRONEOUS OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) GENERAL PURPOSE COMPUTER (GPC)
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [F]

LOCATION: AVIONICS BAY
PART NUMBER: IBM AP-101 CPU / IBM 4P1 IOP

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LACK OF CORRECT OUTPUT FROM THE BFS GPC WILL CAUSE LOSS OF
VEHICLE CONTROL WHEN THE BFS IS ENGAGED. LOSS OF THE
CREW/VEHICLE IS PROBABLE.

REFERENCES: JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 2/1R
MDAC ID: 401 ABORT: 2/1R

ITEM: BFS ENGAGE PUSHBUTTON
FAILURE MODE: FAILS TO CLOSE

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	2/1R
LIFTOFF:	2/1R	TAL:	2/1R
ONORBIT:	2/NA	AOA:	2/1R
DEORBIT:	2/1R	ATO:	2/1R
LANDING/SAFING:	2/1R		

REDUNDANCY SCREENS: A [1] B [F] C [P]

LOCATION: 30V73A5, 30V73A6; L, R ROTATION HAND CONTROLLER
PART NUMBER: MC621-0043-3046 (ROTATION HAND CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, CONTAMINATION, PHYSICAL JAMMING

EFFECTS/RATIONALE:

ONE BFS ENGAGE PUSHBUTTON FAILED OPEN PREVENTS BFS ENGAGE USING
ONE RHC.

FAILURE OF BOTH PUSHBUTTONS CAUSES COMPLETE LOSS OF BFS ENGAGE
CAPABILITY. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 402 ABORT: 3/3

ITEM: BFS ENGAGE PUSHBUTTON
FAILURE MODE: INADVERTENT OPERATION, FAILS TO REMAIN OPEN

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/NA	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [1] B [P] C [NA]

LOCATION: 30V73A5, 30V73A6; L, R ROTATION HAND CONTROLLER
PART NUMBER: MC621-0043-3046 (ROTATION HAND CONTROLLER)

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, PHYSICAL JAMMING

EFFECTS/RATIONALE:

INADVERTENT OPERATION OF ONE OR BOTH ENGAGE PUSHBUTTONS WILL
CAUSE THE BFS TO BECOME ENGAGED.
THIS IS AN EXTREMELY UNDESIRABLE SITUATION. CRITICALITIES HAVE
BEEN ASSIGNED ASSUMING THAT A SMOOTH TRANSITION IS MADE FROM PASS
TO BFS, AND THAT THE BFS PERFORMS AS INTENDED. IF THE FAILURE
OCCURS PRELAUNCH, LAUNCH WILL BE DELAYED OR SCRUBBED.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/2R
MDAC ID: 403 ABORT: 3/3

ITEM: BFC DISENGAGE SWITCH
FAILURE MODE: FAILS TO CLOSE

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/2R	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 34V73A6A5; PANEL F6 A5 S6
PART NUMBER: ME452-0102-7302

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

A "FAILED OPEN" DISENGAGE SWITCH IS A LOSS OF THE NOMINAL MEANS OF DISENGAGING THE BFS. THE OTHER WAY TO DISENGAGE BFS / RE-ENGAGE PASS IS TO RE-IPL PASS GPC'S AND RECYCLE POWER ON THE BFS GPC.

LOSS OF ALL MEANS OF DISENGAGING BFS / RE-ENGAGING PASS WILL IMPACT THE MISSION IF BFS HAS BEEN ENGAGED DURING ASCENT. SAFETY OF THE CREW/VEHICLE IS UNAFFECTED.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 404 ABORT: 1/1

ITEM: BFC DISENGAGE SWITCH
FAILURE MODE: FAILS TO REMAIN OPEN, FAILS TO RE-OPEN

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		HDW/FUNC
	HDW/FUNC	ABORT	
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [NA]

LOCATION: 34V73A6A5; PANEL F6 A5 S6
PART NUMBER: ME452-0102-7302

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

IF THE DISENGAGE SWITCH IS FAILED CLOSED, THE BFS CANNOT BE
ENGAGED. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 405 ABORT: 3/3

ITEM: BFC CRT DISPLAY SWITCH
FAILURE MODE: FAILS TO CLOSE, FAILS TO REMAIN CLOSED

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/NA	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [2] B [P] C [NA]

LOCATION: 35V73A3A1; PANEL C3 A1 S17
PART NUMBER: ME452-0102-7101

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

FAILURE OF THE BFC CRT DISPLAY SWITCH PREVENTS USE OF THE BFC CRT
SELECT SWITCH. A BACKUP MEANS OF ASSIGNING CRT'S TO THE BFS IS
BY KEYBOARD ENTRY.

LOSS OF ALL MEANS OF ASSIGNING A CRT TO THE BFS CAUSES LOSS OF
BFS CRT DISPLAYS PRE-ENGAGE. IF THIS OCCURS PRE-LAUNCH, LAUNCH
WILL BE DELAYED OR SCRUBBED. POST-ENGAGE, BFS WILL CONTROL CRT'S
1 & 2 BY DEFAULT.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 406 ABORT: 3/3

ITEM: BFC CRT SELECT SWITCH
FAILURE MODE: FAILS TO CLOSE, FAILS TO SWITCH, ERRONEOUS OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/NA	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [2] B [P] C [NA]

LOCATION: 35V73A3A1; PANEL C3 A1 S18
PART NUMBER: ME452-0102-7106

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

FAILURE OF THE BFC CRT SELECT SWITCH IS A LOSS OF ONE MEANS OF ASSIGNING CRT'S TO THE BFS. CRT ASSIGNMENT MAY ALSO BE ACCOMPLISHED BY KEYBOARD ENTRY. LOSS OF ALL MEANS OF ASSIGNING A CRT TO THE BFS CAUSES LOSS OF BFS CRT DISPLAYS PRE-ENGAGE. IF THIS OCCURS PRE-LAUNCH, LAUNCH WILL BE DELAYED OR SCRUBBED. POST-ENGAGE, BFS WILL CONTROL CRT'S 1 & 2 BY DEFAULT.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 407 ABORT: 1/1

ITEM: BFS GPC (USUALLY GPC 5) POWER SWITCH
FAILURE MODE: FAILS TO CLOSE, FAILS TO REMAIN CLOSED

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [P] C [F]

LOCATION: 33V73A6; PANEL O6
PART NUMBER: ME452-0102-7301

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

LOSS OF POWER TO THE BFS GPC CAUSES LOSS OF BACKUP FLIGHT SYSTEM SOFTWARE. LOSS OF THE CREW/VEHICLE MAY RESULT. IF THE FAILURE OCCURS PRELAUNCH, LAUNCH WILL BE DELAYED OR SCRUBBED.

REFERENCES:

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 408 ABORT: 1/1

ITEM: BFS GPC (USUALLY GPC 5) OUTPUT SWITCH
FAILURE MODE: FAILS OUT OF "BACKUP"

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/1	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [P] C [F]

LOCATION: 33V73A6; PANEL O6
PART NUMBER: ME452-0102-7306

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION,
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

IF THE BFS GPC OUTPUT SWITCH FAILS OUT OF THE "BACKUP" POSITION,
THE BFS CANNOT BE ENGAGED. LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES:

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 409 ABORT: 1/1

ITEM: BFS GPC (USUALLY GPC 5) MODE SWITCH
FAILURE MODE: INADVERTENTLY IN "HALT"

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) SWITCHES
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	1/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [2] B [P] C [F]

LOCATION: 33V73A6; PANEL O6
PART NUMBER: ME452-0102-7361

CAUSES: SWITCH JAMMED, MECHANICAL SHOCK, VIBRATION, PIECE PART
STRUCTURAL FAILURE, THERMAL STRESS

EFFECTS/RATIONALE:

IF THE HALT CONTACT IS FAILED ON, THE BFS GPC IS PREVENTED FROM
EXECUTING SOFTWARE. VEHICLE CONTROL IS LOST WHEN THE BFS IS
ENGAGED. LOSS OF THE CREW/VEHICLE MAY RESULT.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/1R
MDAC ID: 501 ABORT: 3/1R

ITEM: CIRCUIT BREAKER, 7.5 AMP. - MAIN A (B,C) SUPPLY TO
L(R) DDU
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/1R
LIFTOFF:	3/1R	TAL:	3/1R
ONORBIT:	3/NA	AOA:	3/1R
DEORBIT:	3/1R	ATO:	3/1R
LANDING/SAFING:	3/1R		

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 33V73A14, 33V73A15, 33V73A16; PANELS 014, 015, 016
PART NUMBER: MC454-0026-2075

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

EACH DDU HAS TWO REDUNDANT POWER SOURCES. FAILURE OF TWO CIRCUIT
BREAKERS FOR THE L(R) DDU WILL PREVENT ENGAGE USING THE L(R) RHC.
FAILURE OF ALL FOUR CIRCUIT BREAKERS RESULTS IN A COMPLETE LOSS
OF BFS ENGAGE CAPABILITY.
LOSS OF THE CREW/VEHICLE MAY RESULT.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 502 ABORT: 1/1

ITEM: FUSE F9, 1 AMP. - CNTL BUS AB3 SUPPLY TO DISENGAGE
SWITCH AND BFC MODULES 1A & 1B (HCED & ENGAGE LOGIC)
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	CRITICALITIES		
	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [F]

LOCATION: 34V73A6A5; PANEL F6 A5
PART NUMBER: ME451-0018-0100

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LOSS OF POWER TO BFC MODULES 1A & 1B HCED'S RESULTS IN LOSS OF
ENGAGE CAPABILITY FROM THE LEFT RHC.
LOSS OF POWER TO BFC MODULES 1A & 1B ENGAGE LOGIC CAUSES LOSS OF
ENGAGE/DISENGAGE CAPABILITY FOR GPC'S 1 (PASS) & 4 (PASS). DUAL
CONTROL OF THE VEHICLE MAY RESULT WHEN BFS IS ENGAGED. LOSS OF
THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 503 ABORT: 1/1

ITEM: FUSE F10, 1 AMP. - CNTL BUS AB3 SUPPLY TO
DISENGAGE SWITCH AND BFC MODULE 2A - HCED & ENGAGE LOGIC
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [F]

LOCATION: 34V73A6A5; PANEL F6 A5
PART NUMBER: ME451-0018-0100

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LOSS OF POWER TO BFC MODULE 2A HCED RESULTS IN LOSS OF ENGAGE
CAPABILITY USING THE LEFT RHC.
LOSS OF POWER TO BFC MODULE 2A ENGAGE LOGIC CAUSES LOSS OF
ENGAGE/DISENGAGE CAPABILITY FOR GPC 2 (PASS). DUAL CONTROL OF
THE VEHICLE MAY RESULT WHEN BFS IS ENGAGED. LOSS OF THE
CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 504 ABORT: 1/1

ITEM: FUSE F11, 1 AMP. - CNTL BUS CAL SUPPLY TO
DISENGAGE SWITCH AND BFC MODULES 2B, 3A, 3B - HCED & ENGAGE LOGIC
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	1/1
LIFTOFF:	1/1	TAL:	1/1
ONORBIT:	3/NA	AOA:	1/1
DEORBIT:	1/1	ATO:	1/1
LANDING/SAFING:	1/1		

REDUNDANCY SCREENS: A [1] B [F] C [F]

LOCATION: 34V73A6A5; PANEL F6 A5
PART NUMBER: ME451-0018-0100

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LOSS OF POWER TO BFC MODULES 2B, 3A, & 3B HCED'S RESULTS IN LOSS
OF ENGAGE CAPABILITY USING THE RIGHT RHC.
LOSS OF POWER TO BFC MODULES 2B, 3A, & 3B ENGAGE LOGIC CAUSES
LOSS OF ENGAGE/DISENGAGE CAPABILITY FOR GPC'S 3 (PASS) & 5 (BFS).
THE BACKUP FLIGHT SYSTEM IS INACCESSIBLE. LOSS OF THE
CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820, JSC 12770

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 1/1
MDAC ID: 505 ABORT: 1/1

ITEM: FUSE F49, 3 AMP. - ESS BUS 3AB SUPPLY TO GPC
OUTPUT SWITCHES (BACKUP & NORMAL DISCRETES)
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	HDW/FUNC	CRITICALITIES	HDW/FUNC
PRELAUNCH:	3/3	ABORT	
LIFTOFF:	1/1	RTLS:	1/1
ONORBIT:	3/NA	TAL:	1/1
DEORBIT:	1/1	AOA:	1/1
LANDING/SAFING:	1/1	ATO:	1/1

REDUNDANCY SCREENS: A [1] B [P] C [F]

LOCATION: 33V73A6; PANEL O6
PART NUMBER: ME451-0018-0300

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

LOSS OF POWER TO THE BACKUP AND NORMAL DISCRETES PREVENTS
SELECTION OF A BACKUP GPC. WHEN THE ENGAGE PUSHBUTTON IS
DEPRESSED, ALL GPC'S WILL DISENGAGE. LOSS OF THE CREW/VEHICLE IS
POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/1R
MDAC ID: 506 ABORT: 3/1R

ITEM: FUSE, 3 AMP. - ESS BUS SUPPLY TO BFS GPC (USUALLY
GPC 5) POWER SWITCH
FAILURE MODE: OPEN CIRCUIT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) CIRCUIT PROTECTION
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES

FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/1R
LIFTOFF:	3/1R	TAL:	3/1R
ONORBIT:	3/NA	AOA:	3/1R
DEORBIT:	3/1R	ATO:	3/1R
LANDING/SAFING:	3/1R		

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 33V73A6; PANEL 06
PART NUMBER: ME451-0018-0300

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

THERE ARE THREE REDUNDANT POWER SUPPLIES TO EACH GPC. AN OPEN
CIRCUIT IN ONE SUPPLY CAUSES LOSS OF ONE LEG OF REDUNDANCY. OPEN
CIRCUITS IN ALL THREE POWER SUPPLIES TO THE BFS GPC RESULT IN
LOSS OF THE BACKUP FLIGHT SYSTEM.
LOSS OF THE CREW/VEHICLE IS POSSIBLE.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 601 ABORT: 3/3

ITEM: BFC ENGAGE LIGHT
FAILURE MODE: LOSS OF OUTPUT

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) INDICATORS
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

FLIGHT PHASE	HDW/FUNC	CRITICALITIES	HDW/FUNC
PRELAUNCH:	3/3	ABORT	
LIFTOFF:	3/3	RTLS:	3/3
ONORBIT:	3/NA	TAL:	3/3
DEORBIT:	3/3	AOA:	3/3
LANDING/SAFING:	3/3	ATO:	3/3

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 34V73A2, 34V73A4; PANELS F2 & F4
PART NUMBER: ME452-0061-9105

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

THE CREW RECEIVES SEVERAL INDICATIONS THAT THE BFS HAS BECOME
ENGAGED, INCLUDING BFC LIGHTS, OUTPUT TALKBACKS, CAM DIAGONAL
LIGHTS AND CRT DISPLAY INFORMATION.

FAILURE OF ONE OR BOTH BFC ENGAGE LIGHTS TO INDICATE BFS ENGAGE
HAS NO SERIOUS IMPACT TO THE CREW/VEHICLE OR TO THE MISSION.

REFERENCES: JSC 18820

INDEPENDENT ORBITER ASSESSMENT
ORBITER SUBSYSTEM ANALYSIS WORKSHEET

DATE: 12/01/86 HIGHEST CRITICALITY HDW/FUNC
SUBSYSTEM: BACKUP FLIGHT SYSTEM FLIGHT: 3/3
MDAC ID: 602 ABORT: 3/3

ITEM: BFC ENGAGE LIGHT
FAILURE MODE: INADVERTENT OPERATION

LEAD ANALYST: L.W.HINSDALE/E.E.PRUST SUBSYS LEAD: J.J.EWELL

BREAKDOWN HIERARCHY:

- 1) INDICATORS
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)

CRITICALITIES			
FLIGHT PHASE	HDW/FUNC	ABORT	HDW/FUNC
PRELAUNCH:	3/3	RTLS:	3/3
LIFTOFF:	3/3	TAL:	3/3
ONORBIT:	3/NA	AOA:	3/3
DEORBIT:	3/3	ATO:	3/3
LANDING/SAFING:	3/3		

REDUNDANCY SCREENS: A [1] B [P] C [P]

LOCATION: 34V73A2, 34V73A4; PANELS F2 & F4
PART NUMBER: ME452-0061-9105

CAUSES: MECHANICAL SHOCK, VIBRATION, PIECE PART STRUCTURAL
FAILURE, THERMAL STRESS, CONTAMINATION

EFFECTS/RATIONALE:

THE CREW RECEIVES SEVERAL INDICATIONS THAT THE BFS HAS BECOME
ENGAGED, INCLUDING BFC LIGHTS, OUTPUT TALKBACKS, CAM DIAGONAL
LIGHTS AND CRT DISPLAY INFORMATION.
INADVERTENT OPERATION OF ONE OR BOTH BFC ENGAGE LIGHTS, WHILE
CONFUSING, HAS NO SERIOUS EFFECT ON THE CREW/VEHICLE OR MISSION.

REFERENCES: JSC 18820

APPENDIX D
POTENTIAL CRITICAL ITEMS

<u>MDAC-ID</u>	<u>ITEM</u>	<u>FAILURE MODE</u>
101	POWER SUPPLY A (B,C) TO L(R) RHC	LOSS OF OUTPUT, PARTIAL OUTPUT
201	HALT RELAY	INADVERTENT OPERATION, FAILS TO REMAIN OPEN
202	HALT RELAY	FAILS TO CLOSE
203	HAND CONTROLLER ENGAGE DRIVER	LOSS OF DISCRETE OUTPUT
204	HAND CONTROLLER ENGAGE DRIVER	LOSS OF 28 VDC OUTPUT
205	ENGAGE/DISENGAGE LOGIC	LOSS OF OUTPUT, ERRONEOUS OUTPUT
207	BFC POWER SUPPLY (5 VDC)	LOSS OF OUTPUT, PARTIAL OUTPUT, FAILS OUT OF TOLERANCE
208	POWER UP/DOWN MONITOR LOGIC	INADVERTENT OPERATION
209	POWER UP/DOWN MONITOR LOGIC	LOSS OF OUTPUT
301	BACKUP GPC (USUALLY GPC 5)	LOSS OF OUTPUT
302	BACKUP GPC (USUALLY GPC 5)	ERRONEOUS OUTPUT
401	BFS ENGAGE PUSHBUTTON	FAILS TO CLOSE
403	BFC DISENGAGE SWITCH	FAILS TO CLOSE
404	BFC DISENGAGE SWITCH	FAILS TO REMAIN OPEN, FAILS TO RE-OPEN
407	BFS GPC (USUALLY GPC 5) POWER SWITCH	FAILS TO CLOSE, FAILS TO REMAIN CLOSED
408	BFS GPC (USUALLY GPC 5) OUTPUT SWITCH	FAILS OUT OF "BACKUP"
409	BFS GPC (USUALLY GPC 5) MODE SWITCH	INADVERTENTLY IN "HALT"
502	FUSE F9, 1 AMP. - CNTL BUS AB3 SUPPLY TO DISENGAGE SWITCH AND BFC MODULES 1A & 1B (HCED & ENGAGE LOGIC)	OPEN CIRCUIT
503	FUSE F10, 1 AMP. - CNTL BUS AB3 SUPPLY TO DISENGAGE SWITCH AND BFC MODULE 2A - HCED & ENGAGE LOGIC	OPEN CIRCUIT

MDAC-IDITEMFAILURE MODE

504	FUSE F11, 1 AMP. - CNTL BUS CA1 SUPPLY TO DISENGAGE SWITCH AND BFC MODULES 2B, 3A, 3B - HCED & ENGAGE LOGIC	OPEN CIRCUIT
505	FUSE F49, 3 AMP. - ESS BUS 3AB SUPPLY TO GPC OUTPUT SWITCHES (BACKUP & NORMAL DISCRETES)	OPEN CIRCUIT