

Thermocouple

CP406R0008, (V1.0) PART I  
COMPUTER PROGRAM CONTRACT END ITEM  
BLOCK II  
SPACE SHUTTLE MAIN ENGINE CONTROLLER  
OPERATIONAL PROGRAM

August 11, 1995

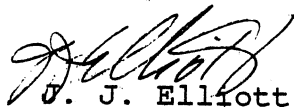
Volume 1, Requirements Text

Version 1.0

PREPARED BY

Rocketdyne Software System Team

APPROVED BY



J. J. Elliott  
Associate Manager  
Controller and Software

RELEASED  
DOCUMENT

MEMORANDUM FOR THE DIRECTOR

Enclosed for the Director are two copies of a letterhead memorandum (LHM) prepared by the Office of the Inspector General (OIG) on 10/15/80. The LHM is dated 10/15/80 and is captioned "Review of the Office of the Inspector General's (OIG) Audit of the Department of Health and Human Services (HHS) Financial Statements for the Fiscal Year 1980." The LHM is a summary of the findings of the audit and is intended to provide the Director with a brief overview of the audit results. The LHM is prepared in accordance with the requirements of the Inspector General Act of 1978, as amended.

Item	Quantity	Unit Price	Total
1. This page intentionally left blank	1	0.00	0.00
2. [Illegible]	1	10.00	10.00
3. [Illegible]	1	20.00	20.00
4. [Illegible]	1	30.00	30.00
5. [Illegible]	1	40.00	40.00
6. [Illegible]	1	50.00	50.00
7. [Illegible]	1	60.00	60.00
8. [Illegible]	1	70.00	70.00
9. [Illegible]	1	80.00	80.00
10. [Illegible]	1	90.00	90.00



MODIFICATIONS SINCE LAST VERSION

The following Requirement Change Notices (RCNs) were incorporated into the Part I Version 2.601 to reflect the change of the HPFT and HPOT Discharge Temperature sensors from RTDs (Resistance Temperature Detectors) to Thermocouples. The resultant thermocouple Part I had its part number and version number changed to CP406R0008 and 1.0 respectively to delineate it from any ensuing Part I based on RTDs. The order of incorporation of the RCNs is shown in the second column.

RCN No.	OR- DER	TITLE AND DESCRIPTION
6164	1	Thermocouple Changes for HPOT and HPFT Discharge Temperatures
6189	3	Correction to RNC 6164 - FID 13 for Last Qualified Sensor Voting for Shutdown
6191	2	Correction to RCN 6164 - Thermocouples, Major Cycle Timing
6239	4	Option to Bypass FASCOS Logic in Thermocouple Software Version
6244	6	Preburner Pump Discharge Temperature Sensor Integrity Monitor Upper Limit
6245	5	Immediate Retry Software Filter for Transient Interrupts
6246	7	Changes to Thermocouple Software
6261	9	Controller Checkout SCP Interrupt Test Erroneous Failure Correction
6262	8	Thermocouple HPOT/HPFT Discharge Temperature Intra-Channel Qualification Test Changes
6273	10	Thermocouple Software Changes to Failure Response and HPOT Discharge Temperature MCF Test

INDEX

This page intentionally left blank

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
1	SCOPE .....	1
1.1	Identification .....	1
1.2	Notation Conventions .....	1
1.2.1	Radix Descriptors .....	1
1.2.2	Word vs. Byte Terminology .....	1
1.2.3	Bit Numbering .....	1
2	APPLICABLE DOCUMENTS .....	2
3	REQUIREMENTS .....	3
3.1	Computer Program Environment .....	3
3.1.1	System Capacities .....	3
3.1.2	Interface Requirements .....	5
3.1.2:1	Interface Block Diagram .....	6
3.1.3	Operational Hardware Description .....	7
3.1.3:1	Digital Computer Unit (DCU) .....	7
3.1.3:1.1	Computer Addressing .....	8
3.1.3:1.2	I/O Addressing .....	9
3.1.3:1.3	MC68000 Exceptions and Interrupt Levels .....	11
3.1.3:1.3.1	Power Failure Interrupt (PFI) .....	13
3.1.3:1.3.2	Power Recovery Interrupt (PRI) .....	13
3.1.3:1.3.3	Self-Checking Pair Interrupt (SCPI) .....	14
3.1.3:1.3.4	Watchdog Timer Halt 1 and 2 Interrupts (WDTH1 and WDTH2) .....	14
3.1.3:1.3.5	Servoactuator Error Indication Interrupt (SEII) .....	14
3.1.3:1.3.6	Timing Reference Interrupt (TRI) .....	14
3.1.3:1.3.7	Redundant Computer Failure Interrupts 1 and 2 (RCFI1 and RCFI2) .....	15
3.1.3:1.3.8	Alternate DCU in Power Failure Interrupt (ADPFI) .....	15
3.1.3:1.4	System Reset .....	15
3.1.3:1.5	Prefetch .....	15
3.1.3:2	Computer Interface Electronics (CIE) .....	16
3.1.3:2.1	Vehicle Interface Electronics (VIE) .....	16
3.1.3:2.1.1	Vehicle to Controller Inputs Via VEEI .....	17
3.1.3:2.1.2	Controller to Vehicle Digital Outputs Via VEEI .....	18
3.1.3:2.2	DCU I/O Interface Electronics .....	19
3.1.3:2.2.1	Watchdog Timers (WDTs) .....	20
3.1.3:2.2.2	Real Time Clock (RTC) .....	20
3.1.3:2.2.3	Failure Data Recorder (FDR) .....	20
3.1.3:2.2.4	Inter-DCU Status Register .....	21

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.1.3:3	Input Electronics (IE)	21
3.1.3:3.1	Input Electronics (IE) Operations	22
3.1.3:3.1.1	Input Electronics DPM System	23
3.1.3:3.1.2	Pulse Rate Data Conversions	23
3.1.3:3.1.3	Analog Data Conversions	23
3.1.3:3.1.4	Sensor Electronics Checkout	24
3.1.3:3.1.5	Propellant Drop Temperature Monitoring	25
3.1.3:3.1.6	Vibration Sensor and Processing Equipment	25
3.1.3:4	Output Electronics (OE)	25
3.1.3:4.1	OE Digital Data Interface	26
3.1.3:4.2	Pneumatic Valve Solenoid Control System	28
3.1.3:4.2.1	Solenoid Coil Drivers	29
3.1.3:4.2.2	Solenoid Monitors	29
3.1.3:4.3	Hydraulic Valve Servoswitch Control System	29
3.1.3:4.3.1	Servoswitch Coil Drivers	30
3.1.3:4.4	Spark Igniter Control System	30
3.1.3:4.4.1	Igniter Command and Power Outputs	30
3.1.3:4.4.2	Igniter Monitors	30
3.1.3:4.5	Hydraulic Servovalve Control System	30
3.1.3:4.5.1	Servovalve Drivers	31
3.1.3:4.5.2	RVDT Position Sensor Monitor	31
3.1.3:4.5.3	Servoactuator Model/Failure Monitor	31
3.1.3:4.6	LVDT Position Sensor Monitor	32
3.1.3:4.7	RVDT and LVDT Excitation Power Supply and Monitor	32
3.1.3:4.8	OE Power Safety Switch	32
3.1.3:4.9	OE Power Monitor Function	33
3.1.3:5	Power Supply Electronics (PSE)	34
3.1.3:5.1	Primary Power Supply System	34
3.1.3:5.2	Backup Power Supply System	36
3.1.3:5.3	Memory Holdup Power Supply	36
3.1.3:5.4	VSPE Power	36
3.2	Operational Program Requirements	37
3.2.1	Executive Processing	37
3.2.1:1	PROM/RAM Program Entry	37
3.2.1:1.1	In-Channel Reset Channel Response	38
3.2.1:1.2	Cross-Channel Reset Channel Response	38
3.2.1:1.3	Receipt of Exit PROM while in PROM	38
3.2.1:1.4	Receipt of Exit PROM while in RAM	39
3.2.1:1.5	In-Channel Power Failure Response	39
3.2.1:1.6	In-Channel Power Recovery Response	40

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.1:2	Major Cycle Control .....	42
3.2.1:2.1	Normal Sequencing .....	42
3.2.1:2.1.1	Input Requirements .....	43
3.2.1:2.1.2	Output Requirements .....	44
3.2.1:2.1.2:1	Inter-DCU Status Register Outputs .....	44
3.2.1:2.1.2:2	Output Electronics Processing .....	44
3.2.1:2.2	Major Cycle Initiation .....	45
3.2.1:2.2.1	Major Cycle Initiation after PROM Exit, Controller Checkout or Controller Reset .....	46
3.2.1:2.2.2	Major Cycle Initiation After PRI .....	48
3.2.1:2.2.3	Completion of Major Cycle Initiation .....	51
3.2.1:2.3	Major Cycle Restart .....	53
3.2.1:3	Watchdog Timer (WDT) Control .....	63
3.2.1:4	Computer Status and Exception Control .....	64
3.2.1:4.1	Computer Exceptions .....	66
3.2.1:5	Exception Processing .....	66
3.2.1:5.1	Reset Exception (PROM) .....	66
3.2.1:5.2	Reset Exception (RAM) .....	66
3.2.1:5.3	Bus Error Exception .....	67
3.2.1:5.4	Address Error Exception .....	67
3.2.1:5.5	Illegal Instruction Exception .....	67
3.2.1:5.6	Zero Divide Exception .....	67
3.2.1:5.7	CHK Instruction Exception .....	67
3.2.1:5.8	TRAPV Instruction Exception .....	67
3.2.1:5.9	Privilege Violation Exception .....	68
3.2.1:5.10	Trace Exception .....	68
3.2.1:5.11	Illegal Exception Vectors .....	68
3.2.1:5.12	Spurious Interrupt Exception .....	68
3.2.1:5.13	TRAP Instruction Exceptions .....	68
3.2.1:5.14	PFI .....	69
3.2.1:5.15	PRI .....	69
3.2.1:5.16	SCPI .....	69
3.2.1:5.17	WDTH1 and WDTH2 .....	69
3.2.1:5.18	SEII .....	69
3.2.1:5.19	TRI .....	69
3.2.1:5.20	RCFI1 and RCFI2 .....	69
3.2.1:5.21	ADPFI .....	69
3.2.1:5.22	CIE Erroneous Acknowledge Level Interrupt .....	70
3.2.1:5.23	Spurious CIE Interrupt .....	70

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.1:6	Disqualification of Controller Components .....	70
3.2.1:6.1	Self-disqualification of DCU/CIE .....	71
3.2.1:6.2	Disqualification of an IE Channel .....	72
3.2.1:6.3	Disqualification of an OE Channel .....	74
3.2.1:6.4	Disqualification of Servoactuators .....	75
3.2.1:6.5	Disqualification of the Cross-Channel DCU/IE/OE .....	77
3.2.1:7	Fault Traceability Provisions .....	78
3.2.1:8	Standby DCU Processing .....	79
3.2.1:8.1	Configuration/Phase/Mode Tracking .....	79
3.2.1:8.2	Component Checkout Mode Tracking .....	85
3.2.1:8.3	OE A and Servoactuator Tracking .....	85
3.2.1:8.4	Control Loop Tracking .....	85
3.2.1:8.5	Standby DCU Sensor Monitoring .....	86
3.2.1:8.6	Standby DCU Monitoring for Ignition Confirmation .....	86
3.2.1:8.7	Standby DCU I/O Operations and Restrictions .....	87
3.2.1:9	Cross-Channel DCU Failure and Power Loss Monitoring .....	87
3.2.1:9.1	DCU B Takeover .....	88
3.2.1:9.1.1	DCU B Takeover Immediate Functions .....	89
3.2.1:9.1.2	DCU B Takeover Major Cycle Functions .....	90
3.2.1:9.2	Failure of DCU B .....	90
3.2.1:9.3	Power Interruption/Loss in Cross-Channel .....	91
3.2.1:9.3.1	Allowance for Power Interruption in the Cross-Channel .....	91
3.2.1:9.3.2	Power Loss After Cross-Channel DCU Disqualification .....	95
3.2.2	Vehicle-Engine Interface .....	96
3.2.2:1	Vehicle Commands .....	97
3.2.2:1.1	Command Recognition and Response .....	98
3.2.2:1.2	Command Voting .....	99
3.2.2:1.3	Command Acceptance and Execution .....	101
3.2.2:1.4	Memory Loading Functions .....	102
3.2.2:2	Vehicle Recording Channel (VRC) Functions .....	102
3.2.2:2.1	Readout Capabilities .....	102
3.2.2:2.1.1	Readout by the PROM Program .....	102
3.2.2:2.1.2	Readout by the Operational Program .....	102
3.2.2:2.2	Vehicle Data Table Transmission .....	107
3.2.2:2.2.1	VDT Contents .....	107
3.2.2:2.2.2	VDT Processing .....	109
3.2.2:2.2.3	Selectable Entries of the VDT .....	110
3.2.2:2.2.4	Control of VDT VRC Transmissions .....	110
3.2.2:2.3	Failure Data Recorder (FDR) Readout .....	112

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.3	Engine Operations .....	113
3.2.3:1	Engine Control and Sequencing Operations .....	113
3.2.3:1.1	Checkout Phase .....	114
3.2.3:1.1.1	Controller Reset .....	114
3.2.3:1.1.2	Checkout Standby Mode .....	115
3.2.3:1.2	Start Preparation Phase .....	117
3.2.3:1.2.1	Purge Sequence One Mode .....	117
3.2.3:1.2.2	Purge Sequence Two Mode .....	117
3.2.3:1.2.3	Purge Sequence Three Mode .....	117
3.2.3:1.2.4	Purge Sequence Four Mode .....	118
3.2.3:1.2.5	Engine Ready Mode .....	118
3.2.3:1.2.6	Start Enable .....	118
3.2.3:1.2.7	Termination of Purges by Command .....	120
3.2.3:1.3	Start Phase .....	120
3.2.3:1.4	Mainstage Phase .....	121
3.2.3:1.4.1	Control Loop Computations .....	121
3.2.3:1.4.2	MCC Pc Control .....	122
3.2.3:1.4.3	Mixture Ratio Control .....	122
3.2.3:1.4.4	Open Loop Control of CCV, MFV, and MOV .....	122
3.2.3:1.5	Shutdown Phase .....	123
3.2.3:1.5.1	Assured Pneumatic Shutdown .....	123
3.2.3:1.6	Post Shutdown Phase .....	124
3.2.3:1.6.1	Terminate Sequence Mode .....	125
3.2.3:1.6.2	Oxidizer Dump Mode .....	125
3.2.3:1.7	Engine On Failure Modes .....	125
3.2.3:1.7.1	Electrical Lockup .....	126
3.2.3:1.7.2	Hydraulic Lockup .....	126
3.2.3:1.7.3	Thrust Limiting .....	127
3.2.3:1.7.4	Fixed Density .....	129
3.2.3:2	Engine Checkout Operations .....	130
3.2.3:2.1	Propellant Drop Monitoring .....	130
3.2.3:2.2	Checkout Standby Mode Tests .....	132
3.2.3:2.2.1	DCU Exception Processing Test .....	132
3.2.3:2.2.2	PSE Output Voltages Maintenance Monitoring Test .....	134

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.3:2.3	Engine Component Checkout .....	136
3.2.3:2.3.1	Sensor Checkout Test .....	138
3.2.3:2.3.2	Igniter Checkout Test .....	140
3.2.3:2.3.3	Pneumatic Component Tests .....	141
3.2.3:2.3.4	Actuator Component Tests .....	142
3.2.3:2.3.5	Controller Checkout Tests .....	144
3.2.3:2.3.5:1	SCP Comparator Test .....	148
3.2.3:2.3.5:2	SCP Interrupt Test .....	153
3.2.3:2.3.5:3	DTACK Monitor/Bus Error Generator Test .....	155
3.2.3:2.3.5:4	VRC DPM Write/Read Test .....	155
3.2.3:2.3.5:5	VRC Output Test .....	156
3.2.3:2.3.5:6	IE DPM Write/Read Test .....	157
3.2.3:2.3.5:7	IE Address Counter Test .....	158
3.2.3:2.3.5:8	IE Range Counter Test .....	159
3.2.3:2.3.5:9	IE Terminate Sequence Test .....	160
3.2.3:2.3.5:10	IE Pulse Rate Converter Control Bit Test .....	161
3.2.3:2.3.5:11	IE Pulse Rate Converter Test .....	162
3.2.3:2.3.5:12	OE Storage Registers Test .....	165
3.2.3:2.3.5:13	D/A and A/D Converter Wraparound Test .....	167
3.2.3:2.3.5:14	Watchdog Timer Counter/Time Reference Interrupt Test .....	167
3.2.3:2.3.5:15	Watchdog Timer Interrupt Test .....	171
3.2.3:2.3.5:16	Watchdog Timer OE Data Switch Test .....	179
3.2.3:2.3.5:17	Watchdog Timer IE Data Switch Test .....	182
3.2.3:2.3.5:18	Watchdog Timer VRC Data Switch Test .....	184
3.2.3:2.3.5:19	OE Power Safety Switch DCU Control Test .....	186
3.2.3:2.3.5:20	OE Power Safety Switch Power Down Matrix Test .....	195
3.2.3:2.3.5:21	OE Power Safety Switch Voltage Monitor/Power Up Reset Test .....	202
3.2.3:2.3.5:22	PSE Power Off Indicator Test .....	210
3.2.3:2.3.5:23	Cross-Channel Power Test .....	210
3.2.3:2.3.5:24	RVDT/LVDT Excitation Power Supply Source Test .....	211
3.2.3:2.3.5:25	Pneumatic Solenoid Test .....	212
3.2.3:2.3.5:26	Servoactuator Error Indication Interrupt Test .....	214
3.2.3:2.3.5:27	Servoactuator Driver Current Test .....	216
3.2.3:2.3.5:28	Failure Data Recorder Test .....	216
3.2.3:2.3.6	Engine Leak Detection Test Support .....	217
3.2.3:2.3.7	Deactivate All Valves .....	220
3.2.3:2.3.8	Actuator Pre-operational Conditioning Cycle .....	220
3.2.3:2.3.9	Hydraulic Conditioning .....	222



TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.3:2.4	Flight Readiness Test (FRT) Configurations .....	223
3.2.3:2.4.1	FRT Operation .....	223
3.2.3:2.4.1:1	FRT Mode .....	224
3.2.3:2.4.1:1.1	FRT-1 .....	224
3.2.3:2.4.1:1.2	FRT-2 .....	225
3.2.3:2.4.1:2	Normal Deactivation of FRT Mode .....	226
3.2.3:2.4.1:3	Off-Nominal Deactivation of FRT Mode .....	226
3.2.3:2.4.2	Engine Simulation .....	227
3.2.3:2.4.3	Failure Simulations .....	228
3.2.3:2.4.3:1	DCU A/OE A and DCU B/OE B Failure Simulations .....	228
3.2.3:2.4.3:1.1	Simulated Disqualification of an OE Channel .....	229
3.2.3:2.4.3:2	Preburner Over-Temperature Simulation .....	230
3.2.3:3	Controller Continual Self-Tests .....	231
3.2.3:3.1	Event Driven Self-Tests .....	232
3.2.3:3.1.1	VEEI Command MUX Self-Test .....	232
3.2.3:3.1.2	CIE Inter-DCU Status Register Self-Test .....	233
3.2.3:3.1.2:1	IDSR Write/Read Check .....	234
3.2.3:3.1.2:2	Determine Pattern (DCU A: React To IDSR B) .....	235
3.2.3:3.1.2:3	Reflect Pattern (DCU B: React To IDSR A) .....	235
3.2.3:3.1.3	VRC Dual Port Memory Self-Test .....	235
3.2.3:3.1.4	Real Time Clock/IE Timing Self-Test .....	235
3.2.3:3.1.5	Interrupt Decoder Self-Test .....	237
3.2.3:3.1.6	IE Sequencer Self-Test .....	238
3.2.3:3.1.7	OE Storage Registers Self-Test .....	239
3.2.3:3.1.8	Watchdog Timer Status Self-Test .....	240
3.2.3:3.2	Periodic Self-Tests .....	240
3.2.3:3.2.1	CIE Data MUX Self-Test .....	240
3.2.3:3.2.2	IE Address and Range Counters Self-Test .....	241
3.2.3:3.2.3	Engine/Controller On/Off Devices Self-Test .....	242
3.2.3:3.2.4	OE Servoactuator Model/Monitor Self-Test .....	244
3.2.3:3.2.5	Interrupt Pending Self-Test .....	246
3.2.3:3.3	IE DPM Data Qualification/Verification Self-Tests .....	247
3.2.3:3.3.1	IE Address and Data Bus Self-Test .....	248
3.2.3:3.3.2	Pulse Rate Converter Self-Tests .....	250
3.2.3:3.3.2:1	2khz RVDT/LVDT Excitation Frequency .....	251
3.2.3:3.3.2:2	HPFP Shaft Speed Sensor .....	252
3.2.3:3.3.2:3	Fuel Flowrate Sensors .....	252
3.2.3:3.3.3	IE Analog to Digital Converter Self-Test .....	252
3.2.3:3.3.4	OE RVDT/LVDT Excitation Power Supply Self-Test .....	254
3.2.3:3.3.5	OE Digital to Analog Converters Self-Test .....	256
3.2.3:3.3.6	PSE Internal Voltages Self-Test .....	257
3.2.3:3.3.7	IE (VSPE) Channel C Power Supply Self-Test .....	258

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.3:4	Engine Sensor Data Processing .....	258
3.2.3:4.1	Sensor Input Data Scaling .....	259
3.2.3:4.2	Sensor Input Data Qualification .....	260
3.2.3:4.2.1	Sensor Input Data Qualification General Rules .....	262
3.2.3:4.2.2	Control Parameter Qualification .....	263
3.2.3:4.2.3	Shutdown Limit Parameter Qualification .....	265
3.2.3:4.2.4	Ignition Confirmation Parameter Qualification .....	268
3.2.3:4.2.5	Propellant Drop Monitoring Parameter Qualification ..	269
3.2.3:4.2.6	Engine Ready Parameter Qualification .....	269
3.2.3:4.2.7	Pogo GOX Flow Check Parameter Qualification .....	269
3.2.3:4.2.8	Vibration Limit Parameter Qualification .....	270
3.2.3:4.2.9	Backdoor Purge Initiation Monitoring Parameter Qualification .....	270
3.2.3:4.2.10	RVDT Monitoring Parameter Qualification .....	270
3.2.3:4.2.11	Purge and Ancillary System Monitoring Parameter Qualification .....	271
3.2.3:4.2.12	GN2/He Purge Monitor Parameter Qualification .....	271
3.2.3:4.2.13	MCC LOX Dome Temperature Parameter Qualification ....	271
3.2.3:4.2.14	Preburner Pump Discharge Temperature Sensor Integrity Monitor Parameter Qualification .....	271
3.2.3:4.2.15	Actuator Settling Check Parameter Qualification .....	272
3.2.3:4.2.16	Cold Junction Temperature Parameter Qualification ...	272
3.2.3:4.3	Sensor/Channel Disqualification .....	272
3.2.3:4.3.1	Temporary Disqualification .....	273
3.2.3:4.3.2	Permanent Disqualification .....	273
3.2.3:4.4	Parameter Computation .....	273
3.2.3:4.4.1	Channel Values .....	274
3.2.3:4.4.2	Control Values .....	275
3.2.3:5	Engine Limit Monitoring .....	277
3.2.3:5.1	Conditions for Engine Ready .....	277
3.2.3:5.2	Ignition Confirmation .....	279
3.2.3:5.3	Shutdown Limit (Redline) Monitoring .....	281
3.2.3:5.3.1	Shutdown Limit (Redline) Failure Responses .....	281
3.2.3:5.4	FASCOS Limit Monitoring .....	282
3.2.3:5.4.1	FASCOS Limit Failure Responses .....	283
3.2.3:5.5	Backdoor Purge Initiation Monitoring .....	284

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.3:6	Engine Component Functions .....	286
3.2.3:6.1	Actuator Data Processing .....	286
3.2.3:6.1.1	Actuator Scaling .....	286
3.2.3:6.1.2	Actuator Command Processing .....	287
3.2.3:6.1.3	Servoactuator Error Indication Interrupt Monitoring .	287
3.2.3:6.1.3:1	Responses to Unscheduled SEII .....	291
3.2.3:6.1.4	RVDT Comparison Test .....	294
3.2.3:6.1.5	Channel B RVDT Monitoring in Start Preparation .....	295
3.2.3:6.1.6	Actuator Exercise Sequence .....	295
3.2.3:6.1.7	Actuator Settling Check .....	297
3.2.3:6.2	Igniter Data Processing .....	298
3.2.3:6.3	Servoswitch and Solenoid Data Processing .....	298
3.2.3:6.4	Purge and Ancillary Systems Monitoring .....	300
3.2.3:6.5	Pogo GOX Flow Check .....	301
3.2.3:6.6	GN2/He Purge Monitor .....	302
3.2.3:6.7	MCC LOX Dome Temperature Monitor .....	302
3.2.3:6.8	Preburner Pump Discharge Temperature Sensor Integrity Monitor .....	302
3.2.3:7	Summary of Engine Control .....	303
3.2.3:7.1	Propellant Valve Control Summary .....	303
3.2.3:7.2	MCC Pc Control Summary .....	305
3.2.3:7.2.1	Thrust Limiting Summary .....	305
3.2.3:7.3	Mixture Ratio Control Summary .....	306
3.2.3:7.3.1	Fixed Density Mode Summary .....	306
3.2.4	Failure Reporting and Responses .....	307
3.2.4:1	Failure Response and Redundancy Management .....	309
3.2.4:2	Failure Reporting .....	311
3.2.4:3	Failure Lists .....	314
3.2.4:4	Failure Response .....	315
3.2.5	Adaptation and Operational Data Constants .....	322
3.2.5:1	Adaptation Data Constants .....	322
3.2.5:2	Operational Data Constants .....	323

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.3	Design Requirements .....	325
3.3.1	Development Requirements .....	325
3.3.2	Design Documentation Requirements .....	325
3.3.3	Coding Standards .....	325
3.3.4	Design Restrictions .....	325
3.3.4:1	Spare Memory and Time .....	325
3.3.4:1.1	Spare Memory .....	325
3.3.4:1.2	Spare Time .....	326
3.3.4:2	Memory Locations Dedicated to PROM .....	326
3.3.4:2.1	Sum Check Address Table (SCAT) .....	326
3.3.4:3	RAM Integrity .....	327
3.3.4:4	Overlays .....	327
3.3.4:5	Verification of Loaded Program .....	327
3.3.4:6	Exception Vector Handling .....	328
3.3.4:7	Computational Precision .....	328
3.3.4:8	Adaptation & Operational Data Design Constraints .....	328
3.3.4:9	Special Patch Software Hook .....	329
3.3.4:10	20 msec VDT .....	329
4	QUALITY ASSURANCE PROVISIONS .....	330
4.1	Development .....	330
4.2	Formal Independent Verification .....	330
5	PREPARATION FOR DELIVERY .....	331
5.1	Object Programs .....	331
5.2	Identification and Marking .....	331
5.3	Program and Concordance Listing .....	331
5.4	Documentation .....	331
5.5	Acceptance/Engineering Verification Data Package .....	332
5.6	Exterior Packaging .....	332
6	NOTES .....	333
6.1	List of Acronyms and Abbreviations .....	333
6.2	Glossary .....	338
6.3	The Tustin Method .....	353

## 1.0 SCOPE

### 1.1 Identification

This specification is Part I of a two-part specification for the Block II SSME Controller Operational Program. It establishes the requirements for performance, design, test and qualification of a Computer Program Contract End Item (CPCEI) identified as the Block II Space Shuttle Main Engine (SSME) Controller Operational Program, (hereafter referred to as the Operational Program). This CPCEI is used to accomplish engine checkout, monitoring, and control, as well as self-test and failure response of the Controller.

### 1.2 Notation Conventions

#### 1.2.1 Radix Descriptors

There are 4 radices used in Part I.

- (a) Hexadecimal (radix 16) numbers are used to denote absolute addresses and word content. This radix is denoted by the prefix \$.
- (b) Decimal (radix 10) numbers are used for all values with units specified. This is the default radix and is not indicated by a prefix.
- (c) Octal (radix 8) numbers are used for Engine Status Word (ESW) and vehicle commands. This radix is denoted by the prefix @. The Failure IDs (FIDs) and Failure Delimiters are octal numbers, but will not be denoted by a prefix.
- (d) Binary (radix 2) numbers are used for describing specific bit patterns not easily represented in either hexadecimal or octal. This radix is denoted by the prefix %.

#### 1.2.2 Word vs. Byte Terminology

Using Motorola's documentation as a guide, byte (8-bit) terminology is used when describing memory address ranges; word (16-bit) terminology when describing instruction lengths; and bytes, words, or long-words (32 bits) as appropriate when describing data.

#### 1.2.3 Bit Numbering

Also using Motorola's documentation as a guide, bits will be numbered from right to left with bit 0 the Least Significant Bit (LSB).

## 2.0 APPLICABLE DOCUMENTS

The following documents of the latest issue form a part of this specification to the extent specified herein.

### SPECIFICATIONS

#### Honeywell

DSCP34053988, Rev C	Block II Space Shuttle Main Engine Controller Flight PROM Software CPCEI (PROM Rev 3)
DSCP34053988, Rev G	Block II Space Shuttle Main Engine Controller Flight PROM Software CPCEI (PROM Rev 5)
DSHG8977A1	Hardware Requirements Specification
DSYG8991A1, Rev R	Hardware/Software Interface Specification

#### Rockwell International

13M15000	Interface Control Document, Space Shuttle Orbiter Vehicle/Main Engine
CP320R0003	Contract End Item Specification, Shuttle Main Engine
RF0001-092	Block II SSMEC Verification Guidelines
RHF-0031-001	Block II SSMEC Software Delivery System Requirements Specification
RSS-8752	Programmers' Handbook for the SSME Block II Controller Software

#### Other

MC68000UM	16-Bit Microprocessor Programmer's Reference Manual Current Edition
-----------	---

### 3.0 REQUIREMENTS

The detailed interface, performance and design requirements describe a computer program that operates within and through a controller as specified by DSHG8977A1 and DSYG8991A1 to control the Space Shuttle Main Engine.

#### 3.1 Computer Program Environment

An SSME controller is composed of two each of the following: a Digital Computer Unit (DCU), a Computer Interface Electronics (CIE), an Input Electronics (IE), an Output Electronics (OE), and a Power Supply Electronics (PSE). Each DCU contains a self-checking pair of MC68000 MPUs (Microprocessing Unit) with their associated main memories. All four MPUs in the controller will execute the same Operational Program.

The Operational Program will be written in a combination of MC68000 assembly language and the "C" programming language. Reference Motorola's MC68000 16-Bit Microprocessor Programmer's Reference Manual, current edition, for a complete description of the assembly language.

##### 3.1.1 System Capacities

The SSME controller contains two DCUs. Each DCU contains a processor composed of two MC68000 MPUs configured as a self-checking pair (SCP). Each MPU has its own main memory and both MPUs execute the same software known as the Operational Program which operates in the following environment:

###### (a) Timing

- (1) Each self-checking pair utilizes an 8 megahertz (Mhz) clock.
- (2) Instruction execution times are as stated in the MC68000 16-bit Microprocessor Programmer's Reference Manual, current edition.
- (3) All engine control, monitoring and required controller management is accomplished 50 times per sec.
- (4) Timing reference interrupts are generated every 5 msec.

3.1.1 System Capacities (Continued)

(b) Main Memory for each MPU

- (1) 128k bytes of alterable memory (volatile RAM).
- (2) 4K bytes of non-alterable memory (PROM).
- (3) The range of Main memory is shown in Table XXXV.

(c) Input/Output (I/O) Addressing

- (1) I/O is memory-mapped as shown in Table XXXV.

(d) Inputs

Inputs to the system comprise vehicle commands, sensors for pressure, temperature, flowrate, shaft speed, actuator position and vibration, digital self-test/calibration words, analog to digital conversions, current and frequency values, power supply data, and input data words from the OE, and an Inter-DCU Status Register.

(e) Outputs

Outputs from the system comprise engine data to the Vehicle Recorder Channels, on/off commands for spark igniters, solenoids, servoswitches, and test parameters, digital to analog conversions, servovalve commands and Inter-DCU Status Register data.

(f) Power

- (1) Three power supply inputs (primary, backup and battery) are provided. The first two inputs are used to support volatile MC68000 registers and RAM. The battery input supplies a hold-up voltage to RAM when both the primary and backup sources are off.
- (2) Each DCU will be able to recover from a 30 msec primary power transient.



### 3.1.2 Interface Requirements

The Block II Space Shuttle Main Engine Controller (SSMEC), when installed on the main engine, operates in conjunction with vehicle command and recorder channels, engine sensors, pneumatic valves, hydraulic actuators, spark igniters, and electrical harnesses to provide a self-contained system for engine control, checkout and monitoring.

To meet the fail-operational and fail-safe design requirements, the controller contains two each of a Digital Computer Unit (DCU A and DCU B), Computer Interface Electronics (CIE A and CIE B), Input Electronics (IE A and IE B), Output Electronics (OE A and OE B), and Power Supply Electronics (PSE A and PSE B). DCU A and CIE A work together as a pair as well as DCU B and CIE B. Each DCU/CIE pair is independent of the other and can perform all of the system requirements. Only one DCU/CIE pair can be in control at any time. In addition, the Vehicle Engine Electrical Interface (VEEI) commands are transmitted on three channels (A, B and C).

Figure 13 shows a block diagram of the controller redundancy necessary to obtain fail-operational and fail-safe performance. In the absence of failures, DCU A will control the inputs from the IEs, the outputs to the OEs, and the inputs from and outputs to the VEEI data channels. If the DCU/CIE A fails, a signal from the timed-out watchdog timer(s) (WDTs) will transfer control of the controller functions to DCU/CIE B, thereby meeting the fail-operational requirement. If DCU/CIE B subsequently fails, the controller will force a Pneumatic Shutdown to meet the fail-safe requirement.

If a DCU/CIE, IE, OE, or power supply fails, the in-control DCU will disqualify the failed component and operate with the remaining components to meet the fail-operational requirement. If both components of the same type fail, the controller will force a pneumatic shutdown to meet the fail-safe requirement.

The controller hardware is specified in DSHG8977A1. The interface between controller hardware and software is specified in DSYG8991A1.

3.1.2:1 Interface Block Diagram

Figures 13 - 17 and 20 - 21 form a set of simplified block diagrams showing the relationship of the DCU, CIE, IE, OE, and Power Supply.

Data from sensors are multiplexed into the IE Dual Port Memories (IE DPMs) where it can be accessed by the DCU. The Operational Program specified herein will reside in main memory, processing the sensor data and providing output commands to the OE as specified herein.

Vehicle commands are validated by the Vehicle Interface Electronics (VIE) portion of the CIE. Engine status is reported to the Vehicle via the Vehicle Recorder Channel Dual Port Memories (VRC DPM) and the Vehicle Recorder Channels (VRC).

### 3.1.3 Operational Hardware Description

Operational hardware comprises the DCU, CIE, IE, OE and PSE.

#### 3.1.3:1 Digital Computer Unit (DCU)

Each of the DCUs contain a Self-Checking Pair Processor (SCP-P), alterable memory, non-alterable memory, comparator logic, a clock oscillator, synchronization and control logic, and an interface bus to its in-channel CIE.

The SCP-P consists of two Motorola MC68000 microprocessors (MPU1 and MPU2), each having its own alterable and non-alterable memory. In addition, each microprocessor in the SCP-P writes to and reads from the Dual Port Memories (DPMs) located in the CIE and receives interrupts from the CIE.

All of the MC68000 instructions defined in MC68000UM are valid, except for the Reset instruction. An SSMEC external devices reset will not occur if the Reset instruction is executed. The Test and Set (TAS) instruction can be executed only within the two usable RAM main memories defined in Table XXXV.

The DCU memory is made up of two identical memory sections, one for each microprocessor in the SCP-P. Each memory contains 128K bytes of alterable memory and 4K bytes of non-alterable memory. In addition, the DCU memory range includes I/O memory.

The DCU SCP microprocessors use memory-mapped I/O to interface with the CIE section of the controller. All inputs to the DCU will be under DCU software control except for the external interrupts. Table XXXV defines the address allocations for alterable main memory (RAM), non-alterable memory (PROM), dual port memory (DPM), and the memory-mapped I/O.

One of the SCP microprocessors is designated as the master microprocessor and the other is designated as the monitor microprocessor. The master microprocessor provides the control interface to the in-channel CIE via its address and data buses. The monitor microprocessor runs the same Operational Program in synchronization with the master microprocessor putting identical values on the address and data buses for transmission to the CIE, as well as to the SCP-P comparator logic. Synchronous operation of the two microprocessors is achieved by using a common clock oscillator to synchronize all microprocessor control signals.

### 3.1.3:1 Digital Computer Unit (DCU) (Continued)

Each DCU has a comparator circuit with two independent comparators. Each comparator does a bit by bit comparison of the master microprocessor's and monitor microprocessor's address and data bus contents for each bus cycle. If a difference is detected by either comparator an SCP (miscompare) Interrupt (SCPI) is generated, the CIE's Failure Data Recorder (FDR) is halted and the watchdog timers are forced to the timed-out state.

The fact that the MC68000 microprocessors are connected as a self-checking pair (SCP) will have no impact on the basic operation of the MC68000. With the exception of the Controller Checkout Test of the self-checking pair comparators, the DCU should be considered as a single computer as far as the Operational Program is concerned.

#### 3.1.3:1.1 Computer Addressing

The MC68000 has the ability to address 16 megabytes of memory. However, only those byte addresses defined in Table XXXV are valid addresses for the Block II SSMEC operation. Any computer access to an invalid address will result in a bus error (BERR) exception and possibly an SCP miscompare.

The 128k byte alterable memory is made up of static Random Access Memory (RAM) and is divided into two blocks of byte addressable memory as follows:

- (a) Lower Block - \$000000 to \$00FFFF
- (b) Upper Block - \$FF0000 to \$FFFFFF

This address partitioning allows memory access of a 64k byte block via the MC68000 address sign extend operation and maintains commonality in the memory board design. Address sign extension is explained in MC68000UM.

The RAM provides alterable storage for DCU instructions, fixed data and temporary data. When utilized, a backup power source external to the controller provides RAM non-volatility.

3.1.3:1.1 Computer Addressing (Continued)

The 4K byte non-alterable memory is composed of semiconductor Programmable Read Only Memory (PROM). The PROM address range is \$800000 to \$800FFF. The PROM provides permanent storage for DCU instructions and fixed data for the functions specified in DSCP34053988, hereafter referred to as the PROM Spec. The PROM is read-only memory and the use of any PROM location as an instruction destination address will result in a bus error (BERR) exception.

During initial power application, AC power interruptions, and upon reception of validated VEEI in-channel Reset Channel commands with Halt Exit enabled, the address bus MSB (bit 23) will be set to 1 and the Reset Exception generated. This will transfer control of the processor to the address contained in the reset vector at location \$800004, placing control within the PROM program.

The PROM will contain at least the following: Power Failure exception processing, Power Recovery exception processing, Bus Error exception processing, Self-Checking Pair exception processing, Illegal Instruction exception processing, RAM Load and Sumcheck routines, PROM Sumcheck routine, Memory and I/O Readout routines, FDR Enable and Readout routines, and Exit PROM routine, as well as, miscompare test words as defined in the PROM Spec.

3.1.3:1.2 I/O Addressing

The DCU I/O is memory-mapped and must be addressed by even (word or long-word) addresses. Any MC68000 instruction that can address memory as an effective address can be used as an I/O instruction with the exception of the Test and Set (TAS) instruction.

The DCU SCP microprocessors use memory-mapped I/O to interface with the Computer Interface Electronics section of the controller. All inputs to the DCU will be under DCU software control except for the external interrupts. Table XXXV defines the address allocations for alterable memory (RAM), non-alterable memory (PROM), DPMS and the memory-mapped direct I/O. Addresses in the range of \$820A00 through \$820DFF are defined as DCU memory-mapped direct I/O addresses.

3.1.3:1.2 I/O Addressing (Continued)

The DCU memory range reserved for direct input commands is defined in Table XXXV as \$820C00 through \$820DFF. Within this range the CIE will decode addresses \$820C00 through \$820CFE. Performing read operations to unused addresses within the range decoded by the CIE will result in undefined data being input to the DCU and possibly an SCP miscompare. Attempting a read operation from any direct I/O address outside the range decoded by the CIE will result in a bus error exception and possibly an SCP miscompare.

The dedicated addresses for direct inputs are defined in Table XXXVI.

The DCU memory range reserved for direct output commands is defined in Table XXXV as \$820A00 through \$820BFF. Within this range, the CIE will decode addresses \$820A00 through \$820AFE. Performing write operations to unused memory addresses within the range decoded by the CIE will result in a no-operation. Attempting a write operation to any direct I/O address outside the range decoded by the CIE will result in a bus error exception.

Direct DCU outputs are defined as either discrete or load operations. Both load and discrete output instructions will use the effective addresses defined in Table XXXVIII as the instruction destination. The discrete output instructions are data independent and activate the output device via address decode; while the load output instructions transfer data to the output device.

Two Dual Port Memories (for IE and VRC) are included in the DCU address space as shown in Table XXXV. Locations within the DPMS may be accessed (at even addresses) in the same manner as main memory locations with the exception of the Test and Set instruction. The operation of the VRC DPM is described in 3.1.3:2.1.2, while that of the IE DPM is described in 3.1.3:3.1.1.

Each CIE has two pairs of DPMS (VRC DPM and IE DPM) for the Vehicle Interface Electronics (VIE) Recorder output data storage and IE sensor data input storage respectively. The address ranges of these DPMS are:

- (a) IE DPM - \$820000 to \$8201FF
- (b) VRC DPM - \$820600 to \$8206FF

3.1.3:1.3 MC68000 Exceptions and Interrupt Levels

The normal processing of the Operational Program can be broken by a category of signals termed exceptions. There are user-defined exceptions which are called interrupts. Each exception has been prioritized by group and priority level, with the interrupts further prioritized by interrupt level. The exceptions generated external to the MC68000 include the Reset and Bus Error exceptions as well as the interrupts. The DCU receives the externally-triggered exceptions from the CIE.

MC68000 Exceptions are divided into 3 different groups:

<u>GROUP</u>	<u>MC68000 EXCEPTION</u>
0	Reset (triggered by System Reset), Bus Error, Address Error, Spurious Interrupt
1	Trace, External User-Defined Interrupts, Illegal Instruction, Privilege Violations
2	TRAP, TRAPV, CHK, Zero Divide

Group 0 exceptions have the highest priority, while Group 2 exceptions have lowest priority. Within Group 0, Reset has highest priority followed by Bus Error, Address Error and Spurious Interrupt. Within Group 1, Trace has priority over external user-defined interrupts, which in turn take priority over Illegal Instruction and Privilege Violation. Group 2 exceptions are generated by instructions. Since only one instruction can be executed at a time, there is no need for a priority relationship within Group 2.

There are 21 different user-defined interrupt sources per DCU/CIE. These 21 interrupt requests are grouped into the seven MC68000 interrupt levels by the CIE interrupt encoder. The exception vector assignments, the group and priority levels, and the interrupt levels for the interrupts are defined in Table XL.

The interrupt encoder utilizes two reserved vectors to trap hardware failures that would cause incorrect exception processing. The CIE Erroneous Acknowledge Level Interrupt is activated whenever the interrupt level acknowledged by the DCU does not equal the interrupt level pending in the CIE interrupt encoder. The Spurious CIE Interrupt is

3.1.3:1.3 MC68000 Exceptions and Interrupt Levels  
(Continued)

activated when the DCU attempts to acknowledge an interrupt when no enabled interrupts are pending in the CIE. These two interrupts can occur at any interrupt level and cannot be disabled in the CIE.

All level 5 through 1 interrupts can be enabled or disabled by individual bits in two CIE Interrupt Mask Registers (see Table XXXIX). In addition, level 6 through 1 interrupts can be enabled or disabled by the appropriate setting of the current interrupt level.

Interrupts are enabled by:

- (a) Setting a mask bit to 1 for each of the appropriate interrupts in the two CIE Interrupt Mask Registers, and
- (b) Setting the current interrupt level to a value less than the level of the interrupts that will be allowed to occur.

Level 7 and 6 interrupts cannot be enabled or disabled by the CIE Interrupt Mask Register. A level 7 interrupt will always occur even if the current interrupt level is set to 7. A level 6 interrupt can be enabled only by setting the current interrupt level to 5 or less.

When interrupts occur their pending status can be detected in Input Words 4 and 7 of Table XXXVII.

Interrupts are disabled by:

- (c) Clearing a mask bit to 0 for each of the appropriate interrupts in the two CIE Interrupt Mask Registers, or
- (d) Setting the current interrupt level to a value equal to or greater than the level of the interrupts that are not allowed to occur.



3.1.3:1.3 MC68000 Exceptions and Interrupt Levels  
(Continued)

When an interrupt is enabled in the CIE, but is prevented from interrupting the MC68000 because of the current interrupt level, the interrupt can be detected by its pending status. When the interrupt is disabled in the CIE, the pending status is set to non-pending.

If an interrupt signal is generated for an interrupt that is disabled either by a mask bit in the CIE or by the current interrupt level, the interrupt, although set (latched), will occur only when the disabling condition is removed.

An interrupt remains set (latched) until its Clear I/O instruction (see Table XXXVIII) is executed. When an interrupt occurs, it should be cleared before the completion of its interrupt response routine to ensure that any further occurrences of the interrupt are related to new events.

All interrupt latches are cleared with the exception of TRI, and all bits of the CIE Interrupt Mask Registers are disabled (cleared) by Master Clear (see 3.1.3:5.1).

A brief description of each of the 21 interrupts follows.

3.1.3:1.3.1 Power Failure Interrupt (PFI)

The Power Failure Interrupt is a level seven interrupt and cannot be disabled from interrupting the Operational Program. PFI is generated by the power supply whenever loss of primary (AC) input power is detected. The power supply will maintain its +5 Vdc outputs for a minimum of 100 usec after a transient is detected to allow an orderly DCU/CIE shutdown.

3.1.3:1.3.2 Power Recovery Interrupt (PRI)

The Power Recovery Interrupt is a level six interrupt. PRI is generated by the power supply when the primary (AC) input power is restored to the nominal operating level, all power supply operating voltage outputs are within specification, and the Power Off Indicator (POI) is not set.

### 3.1.3:1.3.3 Self-Checking Pair Interrupt (SCPI)

The Self-Checking Pair (miscompare) Interrupt is a level five interrupt. The SCPI is generated when the SCP comparators detect a difference in the address or data bits of the two microprocessors of an SCP. The SCPI can be enabled or disabled by a bit in CIE Interrupt Mask Register One. Disabling the SCPI does not prevent an SCP miscompare from timing-out both watchdog timers and inhibiting the FDR recording operation.

### 3.1.3:1.3.4 Watchdog Timer Halt 1 and 2 Interrupts (WDTH1 and WDTH2)

The Watchdog Timer Halt 1 and 2 Interrupts are level four interrupts. These interrupts can be individually enabled or disabled by bits in CIE Interrupt Mask Register One. WDTH1 is generated whenever WDT1 times-out and WDTH2 is generated whenever WDT2 times-out. The WDTH1 and WDTH2 interrupts signal to the in-channel DCU that the WDTs have timed-out and the DCU has failed.

### 3.1.3:1.3.5 Servoactuator Error Indication Interrupt (SEII)

The servoactuator error indications 1 through 12 are level four interrupts. Each of the 12 servoactuator error indications can be enabled or disabled by a corresponding bit in CIE Interrupt Mask Register Two. Six of the 12 error indications are generated by OE A and six are generated by OE B.

A Servoactuator Error Indication Interrupt will be generated by any one of the twelve servoactuator error indications. An input word provides the pending status of the servoactuator error indication which caused the interrupt.

A servoactuator error indication is generated by the demodulated value of the output from the servoactuator RVDT not tracking the servoactuator model within the prescribed limits. The tracking limit for the servoactuator position is  $\pm 6\%$  for Channel A and  $\pm 10\%$  for Channel B.

### 3.1.3:1.3.6 Timing Reference Interrupt (TRI)

The Timing Reference Interrupt is a level three interrupt. The TRI can be enabled or disabled by a bit in CIE Interrupt Mask Register One. The TRI is derived from the real-time clock logic which sets (latches) a timing reference interrupt every  $5000 \pm 5$  usec (nominally 5 msec). This interrupt establishes the timing of the Operational Program's major and minor program cycles.

### 3.1.3:1.3.7 Redundant Computer Failure Interrupts 1 and 2 (RCFI1 and RCFI2)

The Redundant Computer (DCU) Failure Interrupts 1 and 2 are level two interrupts. Both RCFI1 and RCFI2 can be enabled or disabled by bits in CIE Interrupt Mask Register One. RCFI1 and RCFI2 are generated in the cross-channel CIE. RCFI1 is generated by a cross-channel WDT1 time-out and RCFI2 is generated by a cross-channel WDT2 time-out. These signals may occur simultaneously with other cross-channel error indicators, such as ADPFI or a cross-channel SEII.

### 3.1.3:1.3.8 Alternate DCU in Power Failure Interrupt (ADPFI)

The Alternate DCU in Power Failure Interrupt is a level one interrupt. It can be enabled or disabled by a bit in CIE Interrupt Mask Register One. This interrupt is generated by the cross-channel power supply whenever a primary (AC) input power loss is detected.

### 3.1.3:1.4 System Reset

The System Reset signal is generated by either the power supply at turn-on or power recovery, or receipt of an in-channel Reset Channel command while Halt Exit is enabled. When System Reset is received within a DCU, bit 23 of the address bus will be set to 1 to force the Reset Exception to vector address \$800000 instead of address \$000000. Once this address bit has been set to 1, it will remain set until cleared by the software I/O instruction Clear Reset Jam Bit, per Table XXXVIII.

The Reset line of the DCU's microprocessors is not used as an output; thus the Operational Program will not use the MC68000 Reset instruction.

### 3.1.3:1.5 Prefetch

The MC68000 uses a two-word memory prefetch mechanism to improve performance.

The MC68000 fetches two words beyond the current instruction and these words appear on the SCP DCU data buses. When these words appear on the data buses, they are checked by the SCP comparator. Therefore, it is mandatory that the initial memory load routine loads every location in memory with known data to avoid a miscompare when prefetching from an unused address. Additionally, instructions must not be executed from the last two words of low RAM (\$00FFFC, \$00FFFE), PROM (\$800FFC, \$800FFE), and high RAM (\$FFFFFC, \$FFFFFFE) as defined in Table XXXV.

### 3.1.3:1.5 Prefetch (Continued)

Normally the MC68000 prefetches only instructions and not data. However, when the MOVEM instruction is used to move data from memory to registers, the data stream is prefetched to optimize performance. As a result, the processor reads one extra word beyond the higher end of the source area.

Therefore, the same software restrictions applied to the location of instructions due to instruction prefetch, must be applied to the location of MOVEM source data, due to data prefetch. In addition the MOVEM instruction must not be used when fetching from the last two words in either DPM (\$8201FC, \$8201FE and \$8206FC, \$8206FE) or preceding the unused areas of the memory-mapped direct input area (\$820C0C, \$820C0E, \$820C4C, \$820C4E).

### 3.1.3:2 Computer Interface Electronics (CIE)

Each Computer Interface Electronics provides the buffering and control functions necessary to interface its DCU with both IEs, both OEs, and the Vehicle Engine Electrical Interface (VEEI). The two CIEs are identical in function except for the Channel A/B Indicators in the input word described in Table XXXVII.

The CIE is functionally divided into the Vehicle Interface Electronics and the DCU/IO Interface Electronics.

#### 3.1.3:2.1 Vehicle Interface Electronics (VIE)

The Vehicle Interface Electronics provides the digital communication link between the CIE and the Vehicle Engine Electrical Interface (VEEI). The Vehicle Interface Electronics section is divided into four basic functional elements:

- (a) VIE Command and Data Converter,
- (b) VRC DPM,
- (c) VIE Recorder Data Switch,
- (d) VIE Recorder and Data Converter.

### 3.1.3:2.1.1 Vehicle to Controller Inputs Via VEEI

The controller's Vehicle Interface Electronics (VIE) contains three VIE Command and Data Converters which receive control commands or DCU memory load data from the vehicle through the Vehicle Engine Electrical Interface (VEEI).

Each VIE Command and Data Converter tests the validity of each incoming data word. If a data word passes this hardware (BCH) test, the word's 16 bits are stored in the appropriate input command register. If the word fails this hardware test, its data bits are discarded and the appropriate input command register is set to zero.

The Operational Program is responsible for monitoring the three VIE command registers for updates of all incoming commands and data words with the exception of in-channel Reset Channel commands. Whenever hardware detects an in-channel Reset Channel command in two of the three VIE Command and Data Converters and the Halt Exit is enabled, hardware will issue a Reset signal to the in-channel DCU to cause a Reset Exception. The Reset sets address bit 23 which forces the Reset Exception to the vector address of \$800000 (see Table XL), to transfer control of the in-channel DCU to the PROM program.

The Halt Exit for both DCUs will be enabled by the hardware when:

- (a) both DCUs are stopped in RAM
- (b) both DCUs are in PROM, or
- (c) one DCU is stopped in RAM and the other DCU is in PROM.

In all of the above cases the hardware enables (sets to 0) the Halt Exit for both DCUs because with the WDTs timed-out the OE On/Off Registers are cleared, including the Halt Exit. When the Halt Exit is enabled, an in-channel Reset Channel command received while the DCU is in PROM or stopped in RAM will generate a Reset Exception that forces a return to the beginning of the PROM program.

The contents of these command registers may be read by the DCU using the VIE Command Register Channel A/B/C I/O instructions, as defined in Table XXXVI.

### 3.1.3:2.1.2 Controller to Vehicle Digital Outputs Via VEEI

Each VIE Recorder and Data Converter transfers data to the vehicle via the Vehicle Engine Electrical Interface (VEEI). The data is transferred in 128 word blocks and is in the form of Vehicle Data Table (VDT) data, DCU memory readout data, I/O readout data, or Failure Data Recorder (FDR) memory data. The transfers are initiated by the DCU/CIE that has been selected to command the VRC transmissions and which is the source of the VRC data to be transmitted. The rate of transmission is 19 usec per VRC data word. The Operational Program will initiate VRC transmissions in intervals of  $40 \pm 2$  msec.

The Vehicle Interface Electronics output section includes the VIE Recorder Data Switch and the VIE Recorder and Data Converter. The VIE Recorder and Data Converters obtain their input from the VRC DPMS.

Each VIE Recorder and Data Converter is connected to two VRC DPMS via dual VIE Recorder Data Switches. The VIE A Recorder and Data Converter can be connected to the DCU/CIE A master or the DCU/CIE B master microprocessor VRC DPM (#1). The VIE B Recorder and Data Converter can be connected to the DCU/CIE A monitor or the DCU/CIE B monitor microprocessor VRC DPM (#2).

This design allows the VIE A to output master microprocessor data and the VIE B to output monitor microprocessor data. Under normal operation the VIE Recorder Data Switches select the DCU A VRC DPM outputs for transfer on both master and monitor VIEs.

The VIE Recorder Data Switches will select the DCU/CIE B VRC DPMS when either of DCU/CIE A watchdog timers has timed-out or when DCU A executes the Switch VRC to DCU B I/O instruction. The VIE Recorder Data Switches will revert to the DCU/CIE A VRC DPMS when DCU A executes the Switch VRC to DCU A I/O instruction, per Table XXXVIII, provided neither WDT on DCU/CIE A has timed-out. This control of the VIE Recorder Switches allows DCU B Vehicle Data Table and readout data to be output by DCU B while DCU A is controlling the engine. The data in the DCU/CIE B VRC DPMS will be transferred by both master and monitor VIEs.

### 3.1.3:2.1.2 Controller to Vehicle Digital Outputs Via VEEI (Continued)

After the data to be transferred to the vehicle has been stored in the VRC DPMs, the DCU initiates a VRC transmission sequence by executing an Initiate VRC Data Transmission I/O instruction per Table XXXVIII. This initializes each of the VRC DPM address registers (bits 6-0) to 0 and each of the VDT complete bits (bit 7) to 0. The VRC Data Converter fetches the word pointed to by the VRC DPM address register (which ranges from 0 to 127), converts it for output to the vehicle and increments the address register until a count of 127 has been surpassed. This leaves the address register (bits 6-0) cleared to zero with bit 7 set (i.e., a count of 128) to indicate output complete.

The associated address and complete bits are provided in input words per Table XXXVII. For example, VRCA-VDT1A Complete indicates when the VDT from DCU A VRC DPM #1 has been output on VRC A. VRCB-VDT2A Address Register refers to the address register associated with the VDT output from DCU A VRC DPM #2 on VRC B.

VIE A and VIE B operate in parallel such that master and monitor data from the in-control DCU is output simultaneously via the VIE A Recorder and Data Converter and VIE B Recorder and Data Converter respectively during normal dual channel operation.

Because the VRC DPMs are not maintained by the backup (+28 VDC) power supply during a primary power interruption, their contents will not be valid after a power recovery until updated.

### 3.1.3:2.2 DCU I/O Interface Electronics

The DCU I/O interface section of the CIE includes the following functional elements:

- (a) Watchdog Timer (WDT)
- (b) Real Time Clock (RTC)
- (c) Interrupt Level Encoder
- (d) Failure Data Recorder (FDR)
- (e) Halt Exit Control
- (f) I/O Bus Control
- (g) Data Multiplexers
- (h) Input Electronics Dual Port Memories (IE DPMs)
- (i) Inter-DCU Status Register

### 3.1.3:2.2.1 Watchdog Timers (WDTs)

Each CIE contains two watchdog timers (WDTs) which monitor the performance of the in-channel DCU. Failure of the in-channel DCU to update the WDTs will result in the WDTs timing-out and signaling both DCUs of the failure. The WDT time-out generates a Watchdog Timer Halt (WDTH) interrupt to the in-channel DCU and a Redundant Computer Failure Interrupt (RCFI) to the cross-channel DCU. Each of the WDTs generates its own WDTH and RCFI signals. The watchdog timer time-out also generates signals to the IEs, the OEs and the VIEs to transfer control as required. The IE and OE watchdog timer control is such that as long as the DCU/CIE A watchdog timers are in the non-timed-out state, DCU A will control both IEs, OEs, and VRCs (unless Switch VRC is in effect).

The Operational Program can force the WDTs to the timed-out state via the I/O instructions Set WDT1 Time-Out and Set WDT2 Time-Out, per Table XXXVIII. The hardware Master Clear signal (see 3.1.3:5.1) will set the WDTs to the timed-out state.

### 3.1.3:2.2.2 Real Time Clock (RTC)

Each CIE contains a Real Time Clock function that generates Timing Reference Interrupt (TRI) signals at 5 msec intervals. The Real Time Clock counts down from 4999 to 0 with rollover (reset to 4999) occurring at 0.

The Real Time Clock value can be read by means of the RTC I/O instruction as defined in Table XXXVI. The format of this value (RTC Output) is defined in Table XXXVII.

### 3.1.3:2.2.3 Failure Data Recorder (FDR)

Each Computer Interface Electronics contains a Failure Data Recorder that continuously records the address bus data, memory bus data, and control line data of the DCU/CIE monitor microprocessor. The FDR consists of a 2048 by 48-bit RAM, an address counter and control logic.

The FDR recording is initiated by the Enable FDR Recording I/O instruction, per Table XXXVIII. FDR recording is started at FDR memory address 0. During each DCU self-checking pair processor input and output bus cycle, 48 bits of data as defined in Table XXXVII are stored in the FDR memory address pointed to by the FDR address counter. After each bus cycle the FDR address counter is incremented until it reaches the



### 3.1.3:2.2.3 Failure Data Recorder (FDR) (Continued)

last FDR memory address available, \$7FF. After recording data into this address the FDR address counter rolls over to FDR memory address 0. This process of recording data into the FDR memory for each DCU bus cycle continues until inhibited by a DCU self-checking pair miscompare, by the Inhibit FDR Recording I/O instruction per Table XXXVIII, or by a power up reset.

The FDR memory can be read only by the cross-channel DCU. The DCU must verify that the FDR Recording is inhibited (see Table XXXVII) before it executes an FDR read, or the data will not be valid. The in-channel DCU can inhibit the FDR record operation via the Inhibit FDR Recording I/O instruction, per Table XXXVIII.

The FDR memory read will start at the last address recorded unless an AC power off/on cycle has occurred. After an AC power cycle the FDR address may be a value other than the last address recorded. The DCU will read the FDR address and the 48-bit memory word in three 16-bit data groups as defined in Tables XXXVI and XXXVII. This can be repeated until the entire FDR memory has been read.

### 3.1.3:2.2.4 Inter-DCU Status Register

The Inter-DCU Status Registers provide 16-bit communication paths between DCUs. There is one such register per DCU/CIE. An Inter-DCU Status Register can be written into and read by the in-channel DCU/CIE. The cross-channel DCU/CIE may read the other channel's Inter-DCU Status Register.

### 3.1.3:3 Input Electronics (IE)

There are two Input Electronics, IE A and IE B. Each IE provides the interface and signal conditioning between the engine sensors and the CIEs. The IEs also provide the interface for the monitoring of power supply voltages by both DCUs. The output of each IE is cross-strapped to the cross-channel IE DPMS. The IE interface block diagram is shown in Figure 17.

### 3.1.3:3.1 Input Electronics (IE) Operations

The Input Electronics converts analog and pulse rate sensor data into a 16-bit digital format and stores it in the IE DPMs. Sensor data is received from the engine and controller sensors for pressure, temperature, position, voltage level, vibration, rotational speed, flow rate, and frequency.

The in-control DCU initiates an IE input sequence by loading the starting address of a sensor group to be converted into the IE Address Counter via the Load IE Address Counter I/O instruction, loading the number of sensor pairs (minus one) to be converted into the IE Range Counter via the Load IE Range Counter I/O instruction, then starting the IE input sequence via the Initiate IE Operation I/O instruction. These I/O instructions are defined in Table XXXVIII.

The IE Sequencer, upon receiving an Initiate IE Operation I/O instruction, decodes the contents of the address counter and the range counter (which were previously loaded by the in-control DCU) to determine the type of conversion to be made, the number of pairs to be converted, and the IE DPM address in which to store each result. After each pair of data conversions (Channel A and Channel B) has been completed, the IE Sequencer transfers IE A data into the CIE A and CIE B IE DPMs, then transfers IE B data into the IE DPMs. IE DPM address locations for sensor data are defined in Table XXVIII. After the data transfer to IE DPMs is complete, the IE Sequencer increments the address counter and decrements the range counter for the next data conversion. When the range counter equals zero, the IE input sequence is complete and the IE Sequencer is available to the in-control DCU for another IE input sequence. Since each parameter pair conversion takes 50 usec, a complete IE input sequence of 128 pairs requires a nominal 6.4 msec with a maximum of 6.5 msec.

The in-control DCU may terminate an IE input sequence by issuing the Terminate IE Sequence I/O instruction per Table XXXVIII. All sequencing will terminate within 9 usec.

The DCU read or write of IE DPMs has priority over the IE Sequencer write, but will not interrupt an IE Sequencer write in progress. After requesting access to the DPM, the DCU will gain access within 500 nsec.

### 3.1.3:3.1.1 Input Electronics DPM System

The Input Electronics Dual Port Memory System in the CIE consists of two 256 by 16-bit RAMs. The associated control circuits which include range and address counters are located within the IE.

The master IE DPM in each CIE is dedicated to that DCU's master microprocessor. The monitor IE DPM in each CIE is dedicated to that DCU's monitor microprocessor. Both IE DPMs in each CIE receive sensor and monitor data from both IEs.

The IE Sequencer can only perform write operations into the IE DPMs. The IE DPM data content is defined in Table XXVIII.

Because the IE DPMs are not maintained by the backup (+28 VDC) power supply during a primary power interruption, their contents will not be valid after a power recovery until updated.

### 3.1.3:3.1.2 Pulse Rate Data Conversions

Pulse rate data is received by the pulse rate converters (PRC) from engine shaft speed, flow rate sensors and the controller's 2khz power supply.

The pulse rate converters asynchronously convert the time interval between a predetermined number of input pulses into a 15-bit digital word that is stored in a 16-bit buffer register. The converter uses the MSB of the buffer register to indicate new data by inverting the bit for each successive update. The data is input to the IE DPM via an IE input sequence.

### 3.1.3:3.1.3 Analog Data Conversions

Analog data in the form of DC voltage levels is received by the analog data conversion section from engine and controller sensors and voltage monitors. These inputs include:

- (a) Temperature
- (b) Pressure
- (c) Vibration
- (d) Valve position command and actuator position

3.1.3:3.1.3 Analog Data Conversions (Continued)

- (e) D/A Converter output monitors from the OE
- (f) Voltage monitors from the controller internal power supplies and the 115 VAC power buses
- (g) Power Off Indicator voltage monitors from the PSE
- (h) Pneumatic Solenoid Valve voltage monitors from the OE
- (i) Calibration data from the pressure sensor and temperature sensor multiplexers. These fixed inputs are converted into 16-bit digital form and stored in the IE DPMs with pressure and temperature data. The pressure and temperature calibration inputs are defined in Table XXVIII.

The analog data conversion sequence is controlled by the IE Sequencer. The sequencer selects the requested input, channels it to the A/D Converter, initiates the analog to digital conversion, and transfers the A/D converter output to the IE DPMs. Each 16-bit data word transferred to the IE DPM has the 12 MSB generated by the A/D Converter with the 4 LSB always set to %1000.

3.1.3:3.1.4 Sensor Electronics Checkout

The IEs provide the hardware to check out the pressure, temperature, vibration and pulse rate converter electronics.

The pressure and temperature sensor electronics are tested by simulating 80% full-range pressure inputs and 50% full-range temperature inputs.

The vibration sensor electronics are tested by simulating 80% full-range vibration inputs.

The pulse rate converter electronics are tested by switching a 500 hz signal into the PRC sensor inputs.

The controller sensor checkout is controlled by bits in OE On/Off Registers 1A and 1B as defined in Table XXXII. The OE On/Off Register commands are defined in Table XXXI. The OE On/Off storage Register load and transfer I/O instructions are defined in Table XXXVIII. The appropriate bits must be set in both OEs in order to activate this test.

### 3.1.3:3.1.5 Propellant Drop Temperature Monitoring

The IEs provide the hardware to test for the premature presence of propellants in the engine. By switching the gain of the temperature sensor input instrumentation amplifier, the range of the Low Pressure Fuel Pump (LPFP) (T3A/T3B of Table XXVIII) and Preburner Pump Discharge (T4A/T4B of Table XXVIII) temperature sensors will be raised to the ambient range in order to detect cryogenic propellant leakage.

The controller propellant drop gain switch is controlled by bits in the OE On/Off Register 1A and 1B as defined in Table XXXII. The OE On/Off Register commands are defined in Table XXXI. The OE On/Off Storage Register load and transfer I/O instructions are defined in Table XXXVIII. The appropriate bits must be set in both OEs to activate this test.

### 3.1.3:3.1.6 Vibration Sensor and Processing Equipment

Vibration Sensor and Processing Equipment (VSPE) is part of the signal flow utilized to implement the Flight Accelerometer Safety Cut Off System (FASCOS).

There are six accelerometers (vibration sensors) located on the engine; radially mounted, three on the HPOP and three on the HPFP. The three signals for each high pressure pump are input into an associated channel of VSPE. This equipment then performs signal conditioning and outputs four signals into each IE channel for conversion. VSPE Channel C sends its output signals to both IE channels A and B. Reference Figure 19.

See 3.1.3:5.4 for a description of the power supplies used by VSPE.

### 3.1.3:4 Output Electronics (OE)

There are two Output Electronics, OE A and OE B. Each OE provides control to the engine spark igniters, the engine pneumatic valve solenoids, and the engine hydraulic valve servoactuators and servoswitches. The OEs monitor these engine control devices and provide self-test data to both DCUs.

### 3.1.3:4 Output Electronics (OE) (Continued)

The OE is divided into the following functional groups:

- (a) OE Digital Data Interface
- (b) Pneumatic Valve Solenoid Control System
- (c) Hydraulic Servoswitch Control System
- (d) Spark Igniter Control System
- (e) Hydraulic Servovalve Control System
- (f) RVDT and LVDT Excitation Power Supply and Monitor
- (g) OE Power Safety Switch
- (h) OE Power Monitor Function

Both OEs receive digital control commands from the in-control DCU and convert them into discrete and analog voltage signals for interface with engine on/off solenoids and servoswitches, spark igniters, and servovalve actuators. Valve position monitor and test monitor circuits in the OE provide for checking the response of the engine to output commands and the response of the OE to test commands. OE analog data is input to the IE for A/D conversion and storage in the IE DPMs. OE discrete data is input to the CIE data multiplexers and to the CIE interrupt logic.

#### 3.1.3:4.1 OE Digital Data Interface

The OE Digital Data Interface consists of the OE Output Switch, Storage Register, Command Decoder, On/Off Register, and the D/As, as follows:

- (a) OE Output Switch. The OE Output Switch selects control commands from the in-control DCU. Regardless of which DCU is in control, both DCU A and DCU B can perform the monitoring functions associated with both OEs such as reading the digital self-test words for the OE Storage Registers and OE On/Off Registers.

3.1.3:4.1 OE Digital Data Interface (Continued)

- (b) OE Storage Register. The OE Storage Register provides temporary storage for the 16-bit digital commands transferred from the in-control DCU by the Load OE A/B Storage Register I/O instruction. The OE Storage Register contents are transferred to OE On/Off Registers and D/As using the Transfer OE A/B Storage Register I/O instruction. The Load OE A/B Storage Register and Transfer OE A/B Storage Register I/O instructions are defined in Table XXXVIII.
- (c) OE Command Decoder. The OE Command Decoder receives the 4 LSBs of the command stored in the OE Storage Register. The 4 bits are decoded upon execution of the Transfer OE Storage Register I/O instruction to determine which D/A or On/Off Register receives the 12 MSBs of the control command stored in the OE Storage Register, perform servoactuator model/monitor test functions, or change the solenoid monitoring level from Hold to Pull-In by commanding the Solenoid Energize Test, as shown in Table XXXIII.
- (d) Digital to Analog Converters (D/As). There are six D/As in each OE. When the command decoder decodes the 4 LSBs of the OE Storage Register command word as a servovalve command, it will enable the associated D/A to receive the 12 MSBs of the OE Storage Register command word upon execution of the Transfer OE A/B Storage Register I/O instruction per Table XXXVIII. The D/A generates an analog voltage proportional to the digital command for the selected servovalve control system. D/A conversion is defined in Table XXIX. The accuracy and timing of the D/A conversion are defined in DSHG8977A1. Each D/A voltage output is input to the IE for A/D conversion and storage in the IE DPMS, per Table XXVIII. These can be used to verify the servovalve's commanded position. Subsequent to the processing that issues the servovalve commands, a delay of 100 usec is required before the output of the last D/A Value can be requested as an input via the IE input sequence.

The D/A output will be undefined after initial power on and after power interruptions. The Operational Program must command the D/As to a known value before turning on solenoid driver power supplies.

3.1.3:4.1 OE Digital Data Interface (Continued)

- (e) OE On/Off Registers. When the OE Command Decoder decodes the 4 LSBs of the OE Storage Register command word to select an OE On/Off Register, it will enable the associated OE On/Off Register to receive the 12 MSBs of the OE Storage Register command word upon execution of the Transfer OE A/B Storage Register I/O instruction per Table XXXVIII. Table XXXI defines the commands for each of the three OE On/Off Registers.

The OE On/Off Register in conjunction with the OE Command Decoder provides the discrete control signals for the following OE functions:

- (1) On/off control of the engine solenoids and servoswitches.
- (2) Pull-in/hold control of the engine solenoids.
- (3) On/off control of the engine spark igniters.
- (4) On/off control of sensor and propellant drop tests.
- (5) Control of Halt Exit Enable/Disable.
- (6) Cross-channel Power Off Time Exceeded status.

In addition to the OE On/Off Register loading via the Transfer OE A/B Storage Register I/O instruction defined above, the OE On/Off Register is cleared by power up reset during initial power application and during power recovery following momentary interruption.

3.1.3:4.2 Pneumatic Valve Solenoid Control System

The pneumatic valve solenoid control system receives digital commands from the in-control DCU, decodes these commands, and provides the solenoid on/off (energize/deenergize), pull-in, and hold control signals to the engine/controller interface.



### 3.1.3:4.2.1 Solenoid Coil Drivers

The solenoid coil drivers provide +29 VDC (Channel A) or +24 VDC (Channel B) to the controller/ engine interface for solenoid pull-in operation and +16 VDC (Channel A) or +8 VDC (Channel B) for solenoid hold operation. The on/off command bits and the pull-in/hold command bits are in OE On/Off Register 1A for the Channel A solenoids and OE On/Off Register 1B for the Channel B solenoids as defined in Table XXXI. The solenoid driver power supplies in each controller channel are also controlled by the OE Power Safety Switch in each corresponding OE, per 3.1.3:4.8.

NOTE: Commanding any solenoid to the pull-in state will result in all of the solenoids in that channel, which are already commanded on and in the hold state, to revert to the pull-in state. The controller solenoid driver power supply is capable of simultaneously driving at most seven solenoids at the pull-in level.

### 3.1.3:4.2.2 Solenoid Monitors

Hardware monitors the solenoid drive voltage level (SL1 for Channel A, SL2 for Channel B) and the coil current of each solenoid. The solenoid drive voltage level is input to the IE for A/D conversion and storage in the IE DPMs. The solenoid coil current is monitored by a comparator set to generate a logic 0 for each solenoid coil in which the coil current is above the minimum hold level. As long as the solenoid current is above this threshold the solenoid is designated as being energized as denoted in input words per Table XXXVII.

The coil current threshold can be changed to the pull-in level by loading and transferring the Solenoid Energize Test via the OE Storage Register (see Table XXXIII). Once the Solenoid Energize Test is requested, the solenoid coil current comparator will designate the solenoids as being energized only if the current remains above the pull-in level.

### 3.1.3:4.3 Hydraulic Valve Servoswitch Control System

The hydraulic valve servoswitch control system receives digital commands from the in-control DCU, decodes these commands, and provides the fail-operational and fail-safe servoswitch on/off (energize/deenergize) control signals to the controller/engine interface.

Hardware monitors the coil current in each servoswitch coil to provide the status of each servoswitch in input words, per Table XXXVII.

### 3.1.3:4.3.1 Servoswitch Coil Drivers

The servoswitch coil drivers provide +26 VDC to the controller/engine interface for servoswitch operation. The Channel A fail-safe servoswitch on/off command bits are in OE On/Off Register 3A. The Channel B fail-safe servoswitch on/off command bits are in On/Off Register 3B. The fail-operational servoswitch on/off command bits are in OE On/Off Register 2B. OE On/Off Register commands are defined in Table XXXI.

The servoswitch driver power supplies in each controller channel are also controlled by the OE Power Safety Switch in each corresponding OE, as described in 3.1.3:4.8.

### 3.1.3:4.4 Spark Igniter Control System

The spark igniter control system in each OE receives digital commands from the in-control DCU, decodes these commands, and provides +26 VDC power and the on/off (energize/deenergize) control signals to the controller/engine interface for three spark igniters in each channel.

#### 3.1.3:4.4.1 Igniter Command and Power Outputs

The three igniter drives in each OE are commanded on and off simultaneously. The on/off command bit for the Channel A igniters is in OE On/Off Register 1A and for the Channel B igniters is in OE On/Off Register 1B as defined in Table XXXI.

The spark igniter driver power supply is also controlled by the OE Power Safety Switch in the corresponding OE as described in 3.1.3:4.8.

#### 3.1.3:4.4.2 Igniter Monitors

Hardware circuits (three in each OE) monitor each of the six engine spark igniters and provide the status of the igniters in input words, per Table XXXVII.

### 3.1.3:4.5 Hydraulic Servovalve Control System

Each OE contains a servovalve control system for each hydraulically actuated propellant valve. Each control system includes a servovalve driver function, a servoactuator monitor function utilizing the RVDT (Rotational Variable Differential Transformer) position sensor monitor, and a servoactuator model/monitor function.

### 3.1.3:4.5.1 Servo Valve Drivers

The servo valve driver function provides a DC current to the controller/engine interface proportional to the algebraic sum of the servo valve position command from the in-control DCU and the servo valve actuator position feedback signal from the servoactuator monitor function. An IE input sequence transfers this current to the IE DPM as a servo valve current monitor value (see Table XXVIII) which can be used to isolate which servoactuator may have failed. The servo valve driver function is shown in Figure 7, D/A-RVDT Actuator Configuration.

### 3.1.3:4.5.2 RVDT Position Sensor Monitor

The RVDT position sensor monitor utilizes 2 khz excitation. The sensor monitor is used for the servo valve driver function and the servoactuator model/monitor function. The servoactuator positions are input to the IE for A/D conversion and storage in the IE DPMs via an IE input sequence. In the IE DPM these are identified as valve positions for MFV, MOV, CCV, FPOV, OPOV, per Table XXVIII.

### 3.1.3:4.5.3 Servoactuator Model/Failure Monitor

The servoactuator model/monitor compares the model with the actual servo valve position and generates an interrupt (SEII) to both DCUs when the result is out of tolerance.

The servoactuator model/monitor is shown in Figure 7. The model approximates the servoactuator response to the D/A output and sums the result with the RVDT position sensor monitor output. The monitor compares the result of the algebraic summing operation to a predetermined value and generates an interrupt to both DCUs when out-of-tolerance errors are detected. The tolerance level is  $\pm 6\%$  of full scale OPOV actuator position for Channel A and  $\pm 10\%$  of full scale OPOV actuator position for Channel B. The larger error tolerance for Channel B is required to accommodate additional error sources during a servoactuator Channel A to Channel B switchover.

Hardware provides both positive and negative test signals to force an out-of-limit condition at the monitor input to verify the monitor's ability to generate interrupts to the DCUs. These test signals are generated when the commands, Positive Actuator Monitor Test and Negative Actuator Monitor Test, are issued by the in-control DCU via the OE Storage Register as defined in Table XXXIII. The commands apply the negative test input to all servoactuator monitors simultaneously or the positive test input to all servoactuator monitors simultaneously.

#### 3.1.3:4.6 LVDT Position Sensor Monitor

The Linear Variable Differential Transformer (LVDT) position sensor monitor utilizes 2 khz excitation for each of the LVDT position sensors. These are input via an IE input sequence for A/D conversion and storage in the IE DPMS, per Table XXVIII. In the IE DPM these inputs are identified as valve positions for Pogo RIV, Fuel Bleed Valve (FBV), Oxidizer Bleed Valve (OBV) and Anti-Flood Valve (AFV).

#### 3.1.3:4.7 RVDT and LVDT Excitation Power Supply and Monitor

There is one RVDT/LVDT power supply in each OE. The power supply generates a 2 khz excitation signal for the RVDT and LVDT valve position sensors.

The power supply is controlled by OE On/Off Register commands and by the OE Power Safety Switch as described in 3.1.3:4.8.

The 2 khz excitation signal is input to the IE for PRC conversion and storage in the IE DPMS.

#### 3.1.3:4.8 OE Power Safety Switch

Each OE contains an OE Power Safety Switch that provides an alternative way to turn off (in addition to OE On/Off Register control) the in-channel 2 khz excitation, solenoid, servoswitch, and igniter power supplies. The OE Power Safety Switch, in turn, is controlled by the state of the watchdog timers, the OE Power Monitor Function, and the OE Power Control Switch.

DCU A will have control of the OE Power Safety Switches when both its WDTs are reset. DCU B will control the OE Power Safety Switches when either or both of DCU A's WDTs are timed-out. The control of the OE Power Safety Switches by the state of the WDTs (of both DCUs) is called the power down matrix.

The OE Power Monitor Function (see 3.1.3:4.9) detects out-of-tolerance conditions for OE voltages. The OE Power Monitor Function that occurs during initial controller power application and during power recovery following a momentary power interruption is referred to as power up reset.

### 3.1.3:4.8 OE Power Safety Switch (Continued)

The in-control DCU can set (power on) the OE Power Safety Switches by executing the Turn On OE A/B Power Control Switch I/O instructions (see Table XXXVIII). An OE Power Safety Switch is reset (power off) by any one of the following conditions:

- (a) A Turn Off OE A/B Power Control Switch I/O instruction.
- (b) A power up reset operation by the power supply.
- (c) An OE power monitor out-of-tolerance condition.

Both OE Power Safety Switches are reset by the power down matrix when a combination of at least one DCU A WDT and at least one DCU B WDT are in the timed-out state. The power down matrix clears the OE On/Off Registers to the deactivated state on both channels.

### 3.1.3:4.9 OE Power Monitor Function

Each OE contains a power monitor function. The OE Power Monitor Function controls the state of the in-channel 2 khz excitation, pneumatic solenoid, servoswitch, and igniter power supplies, WDT2, and the OE On/Off Registers.

The power monitor function provides the following control functions whenever the Logic +5 VDC or OE +15 VDC power supply voltage is out of tolerance:

- (a) 2 khz excitation, solenoid, servoswitch and igniter power supply outputs are turned off via the reset of the OE Power Safety Switch.
- (b) WDT2 is held in the timed-out state.
- (c) Cross-channel RCFI2 is generated.
- (d) OE On/Off Registers are cleared.

Hardware can simulate a +5 VDC logic power supply under-voltage limit condition to test the power monitor function. The in-channel DCU can activate/deactivate this test by issuing the Set/Reset +5V Under Voltage Test I/O instructions per Table XXXVIII.

### 3.1.3:5 Power Supply Electronics (PSE)

There are two power supply electronics (PSE A and PSE B) that provide power to Channel A and Channel B controller electronics (DCU/CIE, IE, OE) respectively. Each PSE provides control functions to both the in-channel and cross-channel electronics.

Each Power Supply includes a primary power supply, a backup power supply and a RAM memory holdup power supply (battery) in each controller channel.

A set of operator-driven PSE Logic/Redundancy Tests verifies PSE interrupt control logic and controller redundancy operation. The Operational Program provides the necessary functions to support these tests.

#### 3.1.3:5.1 Primary Power Supply System

The primary power supplies provide the DC Voltages required by the controller for normal operation. Each of these power supply outputs are input to the IE for A/D conversion and storage in the IE DPMS, per Table XXVIII Part G.

The primary power supplies generate the following output signals:

- (a) PBD (Power Bus Down) is a discrete logic signal that indicates primary (AC) input power failure. The signal is provided to the cross-channel DCU as Cross-Channel Power Bus Down in an input word per Table XXXVII.
- (b) PFI is an interrupt signal that indicates primary (AC) input power failure to the in-channel DCU.
- (c) PRI is an interrupt signal to the in-channel DCU that indicates operational voltages have recovered from a transient failure condition, and that the Power Off Indicator (POI) is not set.
- (d) ADPFI is an interrupt signal to the cross-channel DCU that indicates primary (AC) input power has failed in the in-channel DCU.
- (e)  $\overline{\text{RESET}}$  is a discrete logic signal that indicates when the power supply outputs have been within the tolerance long enough to support DCU operation after initial power turn-on or after a power transient. It sets address bit 23 and causes a Reset Exception as defined in 3.1.3:2.1.1.

3.1.3:5.1 Primary Power Supply System (Continued)

- (f) Master Clear is a discrete logic signal that instigates initialization when the power supply outputs are within tolerance after initial power turn-on or after a power transient. Master Clear performs the following:
- (1) Clears (resets) the SCP data and address comparators.
  - (2) Resets the IE Channel Indicator (associated with the IE Address Counter) to indicate Channel A.
  - (3) Clears the OE Storage Register to 0.
  - (4) Clears the OE On/Off Registers to the deactivated state; Halt Exit is enabled.
  - (5) Clears the +5 Under Voltage Test to the reset condition.
  - (6) Turns off the OE Power Safety Switch, which deactivates the 2 khz excitation, solenoid, servoswitch and igniter power supplies.
  - (7) Clears (resets) all interrupt latches and pending bits, with the exception of the TRI which remains latched after the other interrupt latches are cleared.
  - (8) Clears the CIE Interrupt Mask Registers, which disables all level 5 through level 1 interrupts.
  - (9) Presets the Real Time Clock to 4999.
  - (10) Clears (sets) WDT1 and WDT2 to the timed-out state.
  - (11) Clears the Inter-DCU Status Register to 0.
  - (12) Resets the VRC switch to DCU A. Clears the address registers to 0 and sets (to 1) the complete bits associated with a VRC transmission sequence.
  - (13) Inhibits FDR recording.

### 3.1.3:5.1 Primary Power Supply System (Continued)

(14) Clears (resets) all PRC counter data to 0.

- (g) POI (Power Off Indicator) is a logic level that is set upon loss of the +28 VDC backup power or the failure of the +5 VDC processor or memory power to remain within the holdup tolerance. The setting of POI inhibits generation of the PRI.

The primary power supplies receive the following signals:

- (h) The OE Power Safety Switch on/off signal controls the 2 khz excitation, solenoid, servoswitch, and igniter power supply outputs as previously described (3.1.3:4.8).
- (i) POI can be set or reset by I/O instructions per Table XXXVIII.

### 3.1.3:5.2 Backup Power Supply System

The backup power supplies provide the DC voltages required to hold up the DCU SCP microprocessors, the RAM main memories, and the RAM FDR memories during primary power supply interruptions. There are no software-controlled functions in the backup power supplies.

### 3.1.3:5.3 Memory Holdup Power Supply

The memory holdup power supplies provide the DC voltage required to hold up the main and FDR memories in the event of both primary and backup input power failures. There are no software-controlled functions in the memory holdup power supplies.

### 3.1.3:5.4 VSPE Power

VSPE Channels A and B obtain power from their associated channel power supplies (i.e., PSE A and PSE B). Power to VSPE Channel C is derived from a combination of power from PSE A and PSE B.

A failure of either PSE A or PSE B would be detected by a PFI or an IE self-test. However, since Channel C of the VSPE is the only element in the IE which utilizes Channel C power, the IE (VSPE) Channel C Power Supply Self-Test (3.2.3:3.3.7) is used to detect power failures that would influence Channel C vibration input values.



### 3.2 Operational Program Requirements

In this section all Operational Program requirements will be stated. Requirements are prefaced by an open bracket, the requirement number, and a closed bracket.

[IR0:1386;1] Except where noted, the detailed requirements of this section shall apply to the Operational Program in both DCU A and DCU B.

The nominal hardware component configuration is as follows:

- (a) DCU/CIE A is the in-control DCU.
- (b) DCU/CIE B is the standby DCU.
- (c) Both IEs, all sensors, and the IE (VSPE) Channel C Power Supply are qualified and all data are utilized.
- (d) Both OEs and their associated servoactuators are qualified.
- (e) Control of the servovalves is by means of the Channel A servoactuators.
- (f) DCU/CIE A commands the VRC transmissions and is the source of the transmitted data.

#### 3.2.1 Executive Processing

##### 3.2.1:1 PROM/RAM Program Entry

Because of the volatile nature of RAM the bootstrap program is in PROM. PROM is entered upon receipt of an in-channel Reset Channel command with Halt Exit enabled, or upon power recovery. The Operational Program disables the Halt Exit so that a Reset Channel command will not take effect while a DCU is cycling, thus preventing a possible occurrence of an SCPI. PROM will be exited and RAM entered upon acceptance of an Exit PROM command. PROM Software requirements are defined in the PROM Spec.

In-channel and cross-channel responses to the Reset Channel and Exit PROM commands are described in the following paragraphs. In addition, in-channel power failure and power recovery responses are provided.

### 3.2.1:1.1 In-Channel Reset Channel Response

If an in-channel Reset Channel command is received while Halt Exit is enabled, control of that DCU is transferred to the PROM by the Reset Exception (see 3.1.3:2.1.1). While in PROM, routines may be utilized to dump or load memory, etc. as stated in 3.1.3:1.1. Control will remain in PROM until receipt of an Exit PROM command. PROM software requirements are defined in the PROM Spec.

If a DCU receives an in-channel Reset Channel command while major cycles are sequencing, the command will be rejected.

### 3.2.1:1.2 Cross-Channel Reset Channel Response

If a DCU receives a cross-channel Reset Channel command while major cycles are sequencing, the command will be rejected.

### 3.2.1:1.3 Receipt of Exit PROM while in PROM

An Exit PROM command received while in PROM will enable the FDR and cause a transition from PROM to RAM.

When the Operational Program is entered from PROM:

- (a) [IR1:1386;1] All interrupts shall be disabled. All SEII monitoring will be suspended (3.2.3:6.1.3).
- (b) [IR2:1386;1] All exception and interrupt vectors used by the PROM program (see the PROM Spec.) shall be initialized to point to their respective service routines in RAM.
- (c) [IR2:4247;1] A Reset +5V under Voltage Test I/O Instruction shall be issued per Table XXXVIII.
- (d) [IR2:2676;1] The RAM Sum Check Address Table (SCAT), described in 3.3.4:2.1, shall be modified so that subsequent sumchecks of RAM will not be performed by PROM.
- (e) [IR2:1386;2] PRI shall be cleared and enabled.
- (f) [IR2:1386;3] SCPI shall be cleared and enabled.
- (g) [IR4:1462;1] This function shall identify the computer as either DCU A or DCU B via the Channel A/B Indicator One/Two per Table XXXVII.

3.2.1:1.3 Receipt of Exit PROM while in PROM (Continued)

- (h) [IR5] The DCU identifier bits in VDT words one and two (i.e., Identification Words one and two) shall be updated.
- (i) [IR6:1386;1] The in-channel DCU shall be assumed to be qualified until its possible disqualification during ensuing processing or self-tests.
- (j) [IR8:1386;1] Existing failure indications and qualification status shall be retained for the IE, OE, servoactuators and sensors.
- (k) [IR9] The functions of Major Cycle Initiation, 3.2.1:2.2, shall be performed.

3.2.1:1.4 Receipt of Exit PROM while in RAM

An Exit PROM command received while in RAM will be accepted and reported but no other action will be taken.

An Exit PROM command will be in the command registers upon entry into RAM from PROM.

3.2.1:1.5 In-Channel Power Failure Response

Power loss is caused by intentional power turn-off or spontaneous interruption. It is indicated to the in-channel DCU by a Power Failure Interrupt (PFI). To the cross-channel, it is indicated by PBD and ADPFI at PFI, RCFI1 and RCFI2 after PFI.

Cross-channel power failure response is defined under 3.2.1:9.3.

[IR17:1386;1] The required response by the in-channel DCU to a PFI while in RAM shall be to perform all necessary preparations for loss of power in the following order:

- (a) [IR20] The in-channel and cross-channel OE power supplies shall be turned off by executing the Turn Off OE A Power Control Switch and Turn Off OE B Power Control Switch I/O instructions, per Table XXXVIII.
- (b) [IR24] The Power Off Indicator (POI) shall be cleared, by executing the Reset POI I/O instruction per Table XXXVIII.

3.2.1:1.5 In-Channel Power Failure Response (Continued)

- (c) [IR24:1843;1] The in-channel watchdog timers (WDT1, WDT2) shall be timed-out by executing the Set WDT1 Time-Out and Set WDT2 Time-Out I/O instructions, per Table XXXVIII, except when the PFI occurs during Checkout Standby. The WDTs are allowed to time-out during Checkout Standby as a support function of the PSE Logic/Redundancy Tests. The tests are conducted only during Checkout Standby.
- (d) [IR27] An MC68000 Stop instruction shall be executed.
- (e) [IR27:1386;1] Following the STOP instruction shall be an MC68000 BRA instruction whose displacement field specifies that the next instruction to be executed is the aforementioned STOP instruction. The BRA ensures that if the Operational Program is restarted, execution will cease with the STOP instruction.

[IR28:588;1] All PFI functions shall be completed in 53 usec, thus allowing 47 usec from PFI to entrance of response request routine (47 + 53 = 100 usec 5 volt holding time).

The required response to PFI when in PROM is given in the PROM Spec.

3.2.1:1.6 In-Channel Power Recovery Response

When controller and DCU power attains (or recovers to) normal operating conditions while POI is not set, it is indicated to the in-channel DCU by a Power Recovery Interrupt (PRI). To the cross-channel DCU it is indicated after a delay of about 1 to 2 usec by the negation of both PBD and the ADPFI signal. However, the ADPFI latch and its pending bit remain set.

Cross-channel power recovery processing is described in 3.2.1:9.3.1.

The required response to PRI by the in-channel DCU while in RAM is to perform all tasks necessary to ensure readiness for reinitialization or a repeat of power loss. They include:

- (a) [IR30] POI shall be set by executing the Set POI I/O instruction per Table XXXVIII.

3.2.1:1.6 In-Channel Power Recovery Response (Continued)

- (b) [IR31:3088;1] Existing phase/mode, failure indications, and qualification status shall be preserved.
- (c) [IR32:4731;1] If the DCU was disqualified prior to power recovery, the DCU shall remain disqualified by performing self-disqualification per 3.2.1:6.1.
- (d) If this is a recovery following a power transient in which the PFI had been non-pending, the DCU will perform self-disqualification per 3.2.1:6.1 (see 3.2.3:3.1.5).
- (e) If phase is Checkout:
  - (1) [IR32:3;1] Verification shall be made that power recovery has cleared the in-channel OE Storage Register to 0 and the in-channel OE On/Off Registers to the deactivated state with Halt Exit enabled. [IR32:4457;1] The verification of the OE On/Off Registers shall exclude the igniters and spares. This procedure is a support function of the PSE Logic/Redundancy Tests.
  - (2) [IR32:3;2] Self-disqualification of the DCU shall be performed per 3.2.1:6.1.
- (f) [IR32:4902;1] If a Major Cycle Initiation was in progress, but was not completed when the PFI/PRI occurred, then the DCU/CIE shall be disqualified per 3.2.1:6.1.
- (g) Otherwise:
  - (1) [IR32:724;1] Recording by the FDR shall be enabled.
  - (2) [IR33] PRI and SCPI shall be cleared, per Table XXXVIII.
  - (3) [IR34] The current interrupt level shall be set to four.
  - (4) [IR35:80;1] Major Cycle Initiation shall be performed, per 3.2.1:2.2.

The required response to PRI while in PROM is given in the PROM Spec.

### 3.2.1:2 Major Cycle Control

The engine control functions and the monitoring functions required of the Operational Program will be iterated at a rate of 50 Hz except where individually specified otherwise. Each iteration is called a major cycle whose period is nominally 20 msec. The major cycle will be initiated and maintained per the following requirements.

#### 3.2.1:2.1 Normal Sequencing

Normal sequencing of the major cycle will be based on the Real Time Clock by synchronizing to the Timing Reference Interrupt (TRI).

[IR36] A TRI is generated every 5 msec and shall mark the beginning of a minor cycle. [IR37] Four minor cycles shall constitute a major cycle.

Sequencing of functions within a major cycle will be designed to achieve efficient processing, engine control, monitoring and response. [IR38] An IE input sequence for the entire IE DPM shall be requested by the in-control DCU in the fourth minor cycle for the following major cycle. [IR39] Scaling of incoming data shall not be initiated by the in-control DCU until the requested sensor data has arrived in the IE DPM and the previous major cycle processing is complete. [IR40:4590;1] Operations requiring scaled data shall be initiated after the applicable incoming data has been scaled. The reasons for beginning sensor input and scaling previous to the major cycle in which this data will be used are to:

- (a) Utilize any spare time at the end of a major cycle for data scaling.
- (b) Allow for non-consecutive major cycles effectively longer than 20 msec.
- (c) Perform VRC transmissions and IE data input concurrently.

[IR41] All control, monitoring and outputs of engine device commands shall be performed in the same major cycle. [IR42] Mission phase/mode shall be changed at either end of the major cycle only, so that all computations (other than data scaling, which is not mode dependent) belong to the same mode. Detailed descriptions of the sequencing of functions will be provided in Part II of this specification. Continual self-tests will be performed every major cycle per subordinate paragraphs of 3.2.3:3.

### 3.2.1:2.1 Normal Sequencing (Continued)

[IR44] Within a major cycle, the required functions shall be sequenced and processed without suspension for intentional synchronization with the minor cycles. The only exceptions are:

- (d) An IE input sequence of sampled engine data will be synchronized with the fourth TRI so that sampling time jitter is minimized.
- (e) Reset of WDTs will be synchronized to the TRI.
- (f) Other functions may be grouped with the items above for convenience or efficiency.

[IR50:1386;1] Time Reference shall be incremented every major cycle, except as explicitly specified elsewhere in this document.

[IR50:1386;2] If the required functions within a major cycle are not completed before receipt of the TRI that designates the start of a new major cycle, the DCU/CIE shall be disqualified per 3.2.1:6.1.

#### 3.2.1:2.1.1 Input Requirements

Parameters are input via the IE DPM every major cycle, per 3.2.1:2.1. An IE input sequence is accomplished by loading the IE Range and Address counters via the Load IE Range/Address I/O instructions, then executing the Initiate IE Operation I/O instruction, per Table XXXVIII.

After the IE input sequence has been completed, the input data can be accessed by fetching it from the IE DPM dedicated addresses, per Table XXVIII. Appropriate IE self-tests of 3.2.3:3 are performed both before and after the IE input sequence to ensure the integrity of the IE.

Discrete input words are read as needed by means of the I/O instructions shown in Table XXXVI.

The Vehicle Command Channel input registers are read as required to meet the response time requirements of 3.2.2, using the VIE Command Register Channel A/B/C I/O instructions shown in Table XXXVI.

The cross-channel Inter-DCU Status Registers A/B (IDSR) are read by using the instructions defined in Table XXXVI. IDSR input will be effected as specified in 3.2.3:3.1.2, CIE Inter-DCU Status Register Self-Test, or 3.2.3:2.3.5, Controller Checkout Tests.

### 3.2.1:2.1.2 Output Requirements

The VRC DPMs must be updated in alternate major cycles per the requirements of 3.2.2:2.

In addition, Inter-DCU Status Register outputs are required as indicated in 3.2.1:2.1.2:1 and OE outputs as indicated in 3.2.1:2.1.2:2.

#### 3.2.1:2.1.2:1 Inter-DCU Status Register Outputs

Data is output to the in-channel Inter-DCU Status Register (IDSR) by using the instructions, per Table XXXVIII. After loading its in-channel IDSR, a DCU will read back the contents and verify the load, per 3.2.3:3.1.2:1. IDSR output will be effected as specified in 3.2.3:3.1.2, CIE Inter-DCU Register Self-Test, or 3.2.3:2.3.5, Controller Checkout Tests.

#### 3.2.1:2.1.2:2 Output Electronics Processing

All commands destined to the D/As or OE On/Off Registers are transferred through the OE Storage Registers. The data destined for the D/A or On/Off Register is packed into the 12 MSBs of a word and the 4 bit code selecting the desired destination into the 4 LSBs. The packed word is then transferred to the storage register using the Load OE A/B Storage Register I/O instruction per Table XXXVIII.

The OE Storage Registers Self-Test of 3.2.3:3.1.7 verifies the proper loading of the storage register before the data is transferred to its intended destination using the Transfer OE A/B Storage Register I/O instruction per Table XXXVIII.

Timing and verification of the D/A outputs will be as specified in 3.2.3:6.1.

The level monitored by the discrete Pull-In/Hold status bit inputs can be changed from Hold to Pull-In by retaining the Solenoid Energize Test code, defined in Table XXXIII, in the OE Storage Register. Use of this I/O instruction is described in 3.1.3:4.2.2 and 3.2.3:2.3.5:25.

The OE On/Off Registers include bits that command functions internal to the DCU, as listed in Table XXXI. These functions include Group 1 and 2 sensor switches, Power Off Time Exceeded, Pull-In/Hold Voltage, PRC Overflow Test, 2 khz Excitation, and Halt Exit. Other bits affect components outside the DCU including igniters, servoswitches, and servoactuators, whose command requirements are defined in 3.2.3:6.



3.2.1:2.1.2:2 Output Electronics Processing (Continued)

The status of all non-spare bits in the OE will be monitored every major cycle by performing the Engine/Controller On/Off Devices Self-Test of 3.2.3:3.2.3.

3.2.1:2.2 Major Cycle Initiation

Major Cycle Initiation is performed to initialize the system with respect to engine control and sequencing upon initial application or reapplication of power. It is also required subsequent to a suspension of major cycle processing for which the WDTs are expected to time-out and/or whenever the major cycle sequence is to be reinitiated.

[IR76:1386;1] The sequence of initiating functions shall include the following:

- (a) [IR76:4795;1] If Major Cycle Initiation is entered from PROM exit, an indication shall be set to perform a Pneumatic Shutdown, per Table XIV, after Major Cycle Restart. [IR76:4795;2] Flight Readiness Test (FRT) mode shall be deactivated. [IR76:4795;3] The memory configuration shall be set to Flight.
- (b) [IR76:4795;4] If Major Cycle Initiation is entered from Controller Checkout, the phase/mode shall be set to Checkout Standby. [IR76:4795;5] The memory configuration shall remain Ground Checkout.
- (c) If Major Cycle Initiation is entered upon receipt of a Controller Reset command, then the phase/mode will have been set to Checkout Standby. [IR76:4795;6] The existing memory configuration shall be retained.
- (d) [IR76:2254;1] If Major Cycle Initiation is entered due to exit from PROM, exit from Controller Checkout, or PRI, the subsequent steps shall be taken:
  - (1) [IR76:1291;1] Both WDTs shall be timed-out by means of the I/O instructions in Table XXXVIII.
  - (2) [IR76:4795;7] Both WDTH interrupts shall be cleared and enabled in the CIE.

3.2.1:2.2 Major Cycle Initiation (Continued)

- (3) [IR76:4905;1] The DCU shall perform self-disqualification (3.2.1:6.1) if either WDT fails to time-out, as determined by the absence of its corresponding WDT interrupt pending bit.
- (e) [IR79:2254;1] RCFI1, RCFI2, and ADPEI shall be disabled (in the CIE), except as necessary in 3.2.1:2.2.1 and 3.2.1:2.2.2, until as indicated under Major Cycle Restart, 3.2.1:2.3. SEII monitoring will be suspended per 3.2.3:6.1.3. [IR79:2979;1] TRI shall be disabled.

The following requirements govern the remainder of the Major Cycle Initiation sequence necessary to select the in-control DCU. Selection of the in-control DCU depends upon the reason Major Cycle Initiation was entered.

3.2.1:2.2.1 Major Cycle Initiation after PROM Exit, Controller Checkout or Controller Reset

[IR84:2254;1] If the Major Cycle Initiation is invoked as a result of:

- (a) PROM exit (invoked as a result of the Exit PROM command), or
- (b) Exit from Controller Checkout, or
- (c) Controller Reset

the subsequent steps shall be performed:

- (d) [IR84:80;1] WDT1 and WDT2 shall be reset.
- (e) [IR84:2168;1] RCFI1 and RCFI2 shall be cleared and enabled in the CIE.
- (f) [IR84:4521;1] If Major Cycle Initiation had been entered from Controller Reset and both RCFIs are negated; or if Major Cycle Initiation had been entered from PROM exit or Controller Checkout, and both RCFIs are negated within 200 msec; then the following shall be performed in the given order:
  - (1) [IR84:2;4] Both RCFIs shall be disabled.

3.2.1:2.2.1 Major Cycle Initiation after PROM Exit,  
Controller Checkout or Controller Reset  
(Continued)

- (2) [IR85:591;1] If the Power Off Time for this channel has been exceeded (per an input word of Table XXXVII), DCU self-disqualification shall be performed (3.2.1:6.1). The primary purpose of the Power Off Time check is to determine if the cross-channel DCU has disqualified the in-channel DCU. This check is also employed as a part of the PSE Logic/Redundancy Tests to determine if the Power Off Time status has failed On into the exceeded state.
  - (3) [IR89:2442;1] Else, if the Power Off Time for this channel has not been exceeded, DCU A shall be declared as the in-control DCU and DCU B shall be declared as the standby DCU; the cross-channel DCU shall be assumed to be qualified; and the cross-channel OE and servoactuator failure indications shall be reset if due to a simulated failure during FRT-1 (3.2.3:2.4.3:1).
- (g) [IR89:4521;1] If neither condition stated in (f) was met, then the following shall be performed in the following order:
- (1) [IR89:1386;2] Both RCFIs shall be disabled, and ADPFI shall be cleared and enabled in the CIE.
  - (2) [IR89:2;5] The in-channel DCU shall be set as the in-control DCU.
  - (3) [IR89:1208;1] If either the ADPFI or the Power Bus Down (PBD) bit indicates power has been lost in the cross-channel, the cross-channel's DCU, IE, and OE shall be disqualified during Completion of Major Cycle Initiation, 3.2.1:2.2.3. [IR89:2;7] Else, if cross-channel power is within tolerance, only the cross-channel DCU shall be disqualified, during Completion of Major Cycle Initiation.
- (h) [IR89:1208;5] Major Cycle Initiation shall be completed per 3.2.1:2.2.3.

3.2.1:2.2.2 Major Cycle Initiation After PRI

Upon power recovery a determination will be made if a full recovery can be attempted, else channel disqualification or shutdown will be performed. In any case memory configuration will be retained as existed prior to the power interruption.

If power recovers and either condition (a) or (b) exists, a complete recovery will be attempted. As part of this recovery the engine phase/mode will be retained as existed prior to the power transient. Operational status for all hardware components will be retained in absence of other disqualifying failures.

- (a) The DCU is not the sole surviving DCU and a PRI occurs in sufficient time for both watchdog timers to be reset in no more than 59.5 msec from the onset of power interruption.
- (b) The DCU is the sole surviving DCU and OPOV travel is not excessive.

Permanent disqualification of the hardware components on the channel experiencing a power interruption will occur, or pneumatic shutdown will be entered under condition (c) or (d) below.

- (c) The DCU is not the sole surviving DCU and a PRI does not occur in sufficient time for both watchdog timers to be reset in no more than 59.5 msec from the onset of power interruption (permanent disqualification). Control by the cross-channel DCU will continue in the current memory configuration and engine phase/mode.
- (d) The DCU is the sole surviving DCU and OPOV travel is excessive (pneumatic shutdown).

If an AC power interruption occurs in less than 440 msec from the previous power recovery on the same channel, the DCU or the DCU, IE, and OE of that channel will be permanently disqualified, or pneumatic shutdown will be entered.

If power is interrupted to a channel whose DCU has previously been disqualified, the IE and OE of that channel will be permanently disqualified.

[IR92] When Major Cycle Initiation has been entered following a PRI, the status of the in-channel DCU and cross-channel DCU shall be determined. [IR93:1265;1] ADPFI, RCFI1 and RCFI2 shall be cleared and enabled in the CIE.

3.2.1:2.2.2 Major Cycle Initiation After PRI (Continued)

[IR93:5083;1] A 500 (-0/+100) usec delay shall be initiated.  
 [IR93:3260;2] If, at any time during the 500 usec delay, there is any indication of RCFI1, RCFI2, ADPFI, or cross-channel power loss via the Cross-Channel Power Bus Down (PBD) status bit, then the cross-channel DCU shall be declared non-operational. [IR93:3260;3] Else the cross-channel DCU shall be declared operational.

Item (e), (f) or (g) below will then be performed depending upon the status of the DCUs.

- (e) [IR93:1386;2] If the cross-channel DCU is operational and the in-channel Power Off Time status is in the exceeded state (per Table XXXVII), the in-channel DCU shall disqualify itself.
- (f) If both DCUs have been determined to be operational and:
  - (1) [IR94:4477;1] If it has been at least 440 +0/-20 msec between the previous power recovery and the last power failure on the in-channel, the following shall occur:
    - (i) [IR95] DCU A shall be declared as the in-control DCU and DCU B as the standby DCU.
    - (ii) [IR96:3300;1] The existing memory configuration and engine phase/mode shall be retained.
    - (iii) [IR98:80;1] The Major Cycle Initiation shall be completed, per 3.2.1:2.2.3.
    - (iv) [IR98:1208;1] Control loop computations (of 3.2.3:1.4.1) shall be bypassed in the first major cycle.
  - (2) [IR98:4477;1] If it has been less than 440 +0/-20 msec between the previous power recovery and the last power failure on the in-channel, the following shall occur:
    - (i) [IR98:1265;2] The in-channel DCU shall disqualify itself, leaving the cross-channel DCU in control.

3.2.1:2.2.2 Major Cycle Initiation After PRI (Continued)

- (g) [IR100:3088;1] If the in-channel DCU has been determined to be operational and the cross-channel DCU has been declared as non-operational, the following shall occur:
- (1) [IR100:3088;2] The in-channel DCU shall be declared as the in-control DCU.
  - (2) [IR100:3088;3] The cross-channel DCU shall be disqualified during Completion of Major Cycle Initiation, 3.2.1:2.2.3. [IR100:4184;1] If the cross-channel DCU is non-operational due to a power loss, then that channel's IE and OE shall also be disqualified during Completion of Major Cycle Initiation, unless previously disqualified.
  - (3) [IR100:4477;1] If at least 440 +0/-20 msec has elapsed between the previous power recovery and the last power failure on the in-channel, and the engine state is Start at Thrust Buildup (Ignition Confirm), Mainstage or Shutdown, the following shall occur:
    - (i) [IR100:3088;6] Indication shall be set to check for OPOV travel due to pneumatic closure. This check will be performed per 3.2.1:2.3(o).
    - (ii) [IR102:3300;1] The existing memory configuration and engine phase/mode shall be retained.
    - (iii) [IR104:80;1] The Major Cycle Initiation shall be completed, per 3.2.1:2.2.3.
    - (iv) [IR104:1394;1] Control loop computations shall be bypassed in the first major cycle.
  - (4) [IR104:4477;1] If less than 440 +0/-20 msec has elapsed between the previous power recovery and the last power failure on the in-channel, or for engine states other than Start after ignition confirmed, Mainstage or Shutdown, the following shall occur:

3.2.1:2.2.2 Major Cycle Initiation after PRI (Continued)

- (i) [IR105] An indication shall be set to perform Pneumatic Shutdown, per Table XIV, subsequent to Major Cycle Restart.
- (ii) [IR106:80;1] The Major Cycle Initiation shall be completed, per 3.2.1:2.2.3.

3.2.1:2.2.3 Completion of Major Cycle Initiation

If the in-channel DCU has not disqualified itself during Major Cycle Initiation, then:

- (a) [IR117:1394;1] WDT1 shall be reset and WDT1 shall be cleared and enabled.
- (b) [IR117:1386;1] WDT2 shall be reset and WDT2 shall be cleared and enabled. [IR117:3088;1] If this sequence was entered from Major Cycle Initiation after PRI, the elapsed time from the Power Off Time Exceeded status check of 3.2.1:2.2.2(e) to the resetting of WDT2 shall not exceed 0.5 msec. This time constraint is required to allow the DCU to restart by resetting both of its WDTs within the race condition window established by the surviving DCU, per 3.2.1:9.3.1(f) (3).
- (c) [IR117:3260;1] If the cross-channel DCU is to be disqualified, the following shall be performed immediately after the resetting of WDT2:
  - (1) [IR117:3260;2] The appropriate OE On/Off Register bit shall be set to indicate Power Off Time in the cross-channel has been exceeded.
  - (2) [IR117:3260;3] The OE Storage Registers Self-Test, 3.2.3:3.1.7, shall be bypassed for this update. The cross-channel Power Off Time Exceeded indication will be set by loading the cross-channel OE Storage Register and immediately transferring the contents.

3.2.1:2.2.3 Completion of Major Cycle Initiation  
(Continued)

- (3) The Engine/Controller On/Off Devices Self-Test, 3.2.3:3.2.3, will be performed. If the in-channel DCU fails to set the Power Off Time Exceeded bit, that DCU will perform self-disqualification. [IR117:3260;4] During such a disqualification, the time between the resetting of WDT2 (above) and the fast time-out of the WDTs, per 3.2.1:6.1, shall not exceed 495 usec.
- (d) [IR117:2442;1] If the in-channel DCU is the in-control DCU, it shall disable Halt Exit for both DCUs.
- (e) [IR117:3235;1] If Major Cycle Initiation occurred because of a PRI, and its preceding PFI had interrupted the disqualification of a component, that component disqualification shall be completed; however, a Major Cycle Restart due to the disqualification shall not be performed. Major Cycle Restart will be invoked as specified below.
- (f) If it has been previously determined that the cross-channel DCU, or cross-channel DCU/IE/OE must be disqualified, the disqualification will now occur per 3.2.1:6.5. A Major Cycle Restart due to the disqualification will be invoked as specified below.
- (g) [IR117:3088;2] If Major Cycle Initiation occurred because of a PRI, an in-channel power recovery shall be reported with the associated failure response.
- (h) [IR118] A Major Cycle Restart shall be performed per 3.2.1:2.3.



3.2.1:2.3 Major Cycle Restart

Major Cycle Restart functions are as follows:

- (a) SEII Monitoring will be suspended (3.2.3:6.1.3). [IR120:2979;1] TRI shall be disabled.
- (b) [IR123:3528;1] All strike counts shall remain unchanged by the Major Cycle Restart.
- (c) [IR124:1394;1] WDT2 shall be reset.
- (d) [IR127:82;1] If Major Cycle Restart was entered from Major Cycle Initiation and the in-channel DCU is the in-control DCU, then the following shall apply:
  - (1) [IR127:3528;1] If an OE or servoactuator channel is disqualified, then the OE Power Control Switch and the OE On/Off Registers shall be commanded to the appropriate state as described in 3.2.1:6.3 or 3.2.1:6.4, respectively.
  - (2) [IR127:2168;1] For qualified OEs, the OE Power Control Switch shall be commanded On, and the source of RVDT/LVDT excitation shall be selected according to the servoactuator channel qualification status. [IR127:1843;1] In addition, the OE On/Off Registers shall be commanded to the following temporary configuration, which shall remain in effect until updated in the first major cycle:
    - (i) [IR127:82;5] All igniters, solenoids, and servoswitches shall be deenergized, with the contingent exception in (ii), below.
    - (ii) [IR127:4641;1] If Major Cycle Restart was entered from Major Cycle Initiation after PRI, then the commanded state of the Emergency Shutdown Solenoid and the HPOP IMSL Purge Solenoid shall remain unchanged.

3.2.1:2.3 Major Cycle Restart (Continued)

(e) [IR127:5672;1] If Major Cycle Restart was entered either from Major Cycle Initiation or because the cross-channel has recovered from a power transient, then the following shall apply:

(1) IR127:5672;2] The IE DPM locations dedicated to the PRC data of shaft speed and flowrate shall be set to \$0000 to prevent the occurrence of an SCPI when these locations are read.

(2) [IR127:5672;3] If the in-channel DCU is in control, the OPOV, FPOV, MFV, MOV, and CCV commands shall be initialized to their last computed commands.

This will allow the Servo-Actuator Model to start recovery from indeterminate values that may be present in the Digital to Analog command registers. For power transients, 57 msec (worst case) are needed from command initialization to enabling SEIIs.

Since the fail-safe servoswitches are deenergized, the actuators are hydraulically locked, preventing these commands from moving the actuators. New actuator commands will be issued per 3.2.1:2.3(i).

(f) [IR127:3235;1] If the in-channel DCU is in control, a Terminate IE Sequence I/O instruction shall be executed, and

(1) If Major Cycle Restart was entered subsequent to a recoverable power transient on either channel, then,

(i) [IR128:1394;1] If the power transient was on the in-channel, power recovery shall be considered the time of the PRI.

[IR128:1208;2] Else, the power transient was on the cross-channel, and power recovery shall be considered the time at which cross-channel power was detected, (per 3.2.1:9.3.1(f)).

(ii) [IR128:1394;3] WDT1 shall be reset.

(iii) [IR128:1386;1] An input of TRCA/TRCB data shall be initiated between 4.0 and 9.0 msec after power recovery.

3.2.1:2.3 Major Cycle Restart (Continued)

- (iv) [IR128:4597;1] All other processing shall be suspended until at least 10.0 msec after power recovery. The 10 msec delay is required for RVDT position settling time. [IR128:1208;3] After the delay, TRI shall be cleared and enabled.
  - (v) [IR128:1386;3] Upon the occurrence of a TRI at least 10.0 msec after power recovery, WDT1 and WDT2 shall be reset. [IR128:1208;4] An IE input sequence of the entire IE DPM shall be initiated.
  - (vi) [IR128:1394;7] The new major cycle shall start upon the TRI following the initiation of the IE input sequence.
  - (vii) [IR128:5501;1] The data for HPFP Shaft Speed, LPFP Shaft Speed, LPOP Shaft Speed and Fuel Flowrate shall not be used for any processing (other than scaling and reporting in the VDT) until the data has been updated by an IE input sequence that occurs at least 20.0 msec after power recovery except as noted in 3.2.3:3.3.2.
  - (viii) [IR128:5501;2] The data for Fuel Bleed Valve, Oxidizer Bleed Valve, Pogo RIV, and Anti-Flood Valve shall not be used for any processing (other than scaling and reporting in the VDT) until the data has been updated by an IE input sequence that occurs at least 40.0 msec after power recovery except as noted in 3.2.3:4.2.4(c).
- (2) Else, if Major Cycle Restart was entered due to a controller component disqualification which switched the source of the 2 khz excitation, then:
- (i) [IR128:3235;1] An input of TRCA/TRCB data shall be initiated at least 1.75 msec after the switch of excitation source. This time is required for 2 khz and related filters to settle within tolerances.
  - (ii) [IR128:3280;1] All other processing shall be suspended until at least 1.0 msec after the request for TRCA/TRCB input data. [IR128:3235;3] After the delay, TRI shall be cleared and enabled.

3.2.1:2.3 Major Cycle Restart (Continued)

- (iii) [IR128:3235;4] Upon occurrence of a TRI, WDT1 shall be reset. [IR128:3235;5] IE input sequence of the entire IE DPM shall be initiated.
  - (iv) [IR128:3235;6] A new major cycle shall start upon the TRI following the initiation of the IE input sequence.
- (3) Else, if Major Cycle Restart was entered due to a DCU B takeover, then,
- (i) [IR128:4184;1] WDT1 shall be reset.
  - (ii) [IR128:5546;1] An input of TRCA/TRCB data shall be initiated between 4.0 and 9.0 msec after commanding On the OE Power Control Switch.
  - (iii) [IR128:5546;2] All other processing shall be suspended until at least 10.0 msec after commanding On the OE Power Control Switch. The 10.0 msec delay is required for RVDT position settling time. [IR128:4184;4] After the delay, TRI shall be cleared and enabled.
  - (iv) [IR128:5546;3] Upon occurrence of a TRI at least 10.0 msec after commanding On the OE Power Control Switch, WDT1 and WDT2 shall be reset. [IR128:4184;6] An IE input sequence of the entire IE DPM shall be initiated.
  - (v) [IR128:4184;7] The new major cycle shall start upon the TRI following the initiation of the IE input sequence.
- (4) Else, Major Cycle Restart had been entered for some reason other than (1), (2), or (3) above, then,
- (i) [IR128:1208;5] TRI shall be cleared and enabled. [IR128:1208;6] Processing shall be delayed until the next TRI; then WDT1 shall be reset and an IE input sequence of the entire IE DPM shall be initiated.

3.2.1:2.3 Major Cycle Restart (Continued)

- (ii) [IR128:1394;9] A new major cycle shall start upon the TRI following the IE input sequence initiation.
- (iii) Because the OE Power Control Switch is turned on as a result of exiting PROM, or subsequent to Controller Checkout, appropriate delays are required for the settling time of the OE 2khz excitation as provided in 3.2.3:3.3.4.

Else, the in-channel DCU is in standby; and

- (5) If Major Cycle Restart was entered either from Major Cycle Initiation after PRI (i.e., subsequent to an in-channel power recovery) or because the cross-channel has recovered from a power transient:
  - (i) [IR128:4912;1] Processing shall be suspended for 25 +/-1 msec to allow the in-control DCU to update the IE DPM. [IR128:4912;2] During this delay WDT1 and WDT2 shall not be timed out.
  - (ii) [IR128:1208;7] TRI shall be cleared and enabled. [IR128:1394;11] Processing shall be delayed until the next TRI; then WDT1 and WDT2 shall be reset.
  - (iii) [IR128:1394;12] The new major cycle shall start upon the subsequent TRI.
- (6) Else, if Major Cycle Restart was not entered as a consequence of power recovery then:
  - (i) [IR128:1208;8] TRI shall be cleared and enabled. [IR128:1394;13] Processing shall be delayed until the next TRI; then WDT1 shall be reset.
  - (ii) [IR128:1394;14] The new major cycle shall start upon the subsequent TRI.
- (g) [IR128:82;1] Prior to commanding or reading data from either OE in the first major cycle, the following shall be performed:

3.2.1:2.3 Major Cycle Restart (Continued)

- (1) If Major Cycle Restart was entered from Major Cycle Initiation, and the in-channel DCU is the in-control DCU, then the OE On/Off Registers will have been previously updated to the qualification status of output devices, as specified in (d).
- (2) [IR128:3088;1] If Major Cycle Restart had not been entered from Major Cycle Initiation and the in-channel DCU is the in-control DCU, the OE On/Off Registers shall be rewritten to reflect phase/mode and the qualification status of output devices.

Writing into the OE On/Off Registers ensures performance of the OE Storage Registers Self-Test prior to execution of other OE self-tests. This will result in disqualification of the cross-channel OE, in the event of an undetected power failure in the cross-channel.

- (h) [IR132:2442;1] The following functions shall be performed in the first major cycle, prior to sensor data processing (independent of scaling):
  - (1) [IR132:1394;1] If the cross-channel DCU is qualified, then RCFI1 and RCFI2 shall be cleared and enabled. [IR132:3494;1] If both DCUs are operational, the IDSR self-test shall be initiated per 3.2.3:3.1.2 if it had been suspended.
  - (2) [IR132:1208;2] If the cross-channel DCU is disqualified, and cross-channel power is operational, then, ADPFI shall be cleared and enabled, per 3.2.1:9.
- (i) Initialization of actuator commands to either prior actuator commands or currently observed positions will occur if Major Cycle Restart was entered due to a power recovery or DCU B takeover, respectively.
  - (1) [IR136:4291;1] If Major Cycle Restart was entered due to a power recovery on either channel, the in-control DCU shall then perform the following:

3.2.1:2.3 Major Cycle Restart (Continued)

- (i) [IR136:4291;2] The OPOV, FPOV, MFV, MOV, and CCV commands shall be initialized to their respective actuator commands that existed just prior to the power transient.
  - (ii) If their respective integral control is in effect, integrators of the MCC Pc and Mixture Ratio control loops will be maintained as existed prior to the power transient.
  - (iii) The MOV control loop (lag) will be maintained as existed prior to the power transient.
- (2) [IR136:4184;1] If Major Cycle Restart was entered due to a DCU B takeover, all actuator commands and active actuator controls shall be initialized according to the observed actuator positions. This will be accomplished in the first major cycle in which RVDT/LVDT excitation is qualified. If RVDT/LVDT excitation is permanently disqualified as a consequence of successive failures of the OE RVDT/LVDT Excitation Power Supply Self-Test, the OE on which the failure was detected will be disqualified, per 3.2.3:3.3.4.

[IR136:2092;1] Subsequent to performance of the OE RVDT/LVDT Excitation Power Supply Self-Test, if RVDT/LVDT excitation is qualified for the controlling actuator channel in either the first or second major cycle, all active control loops shall be initialized in the major cycle in which RVDT/LVDT excitation is first qualified, by performing steps (i)-(iii), below.

- (i) [IR136:1974;2] The OPOV, FPOV, MFV, MOV and CCV commands shall be initialized to their respective RVDT positions.
- (ii) [IR136:1394;5] If their respective integral control is in effect, integrators of the Main Combustion Chamber Pressure in the chamber (MCC Pc) and Mixture Ratio control loops shall be initialized to obtain OPOV and FPOV commands equal to their RVDT positions.

3.2.1:2.3 Major Cycle Restart (Continued)

- (iii) [IR136:1394;6] The MOV control loop (lag) shall be initialized to represent that the value has been steady at its RVDT position.

When position commands have been issued to all servoactuators, fail-safe servoswitches will be commanded to the state described in Servoswitch and Solenoid Data Processing (3.2.3:6.3). The above requirements preclude the possibility of actuator valves being driven to random positions due to indeterminate values in the Digital to Analog Converters.

- (j) [IR136:82;2] In the first major cycle, if closed loop Mixture Ratio control is in effect, Pc Reference shall be set to the current value of MCC Pc (if qualified), or the last value of MCC Pc used for control (if the current value is not qualified).
- (k) [IR136:5192;1] In the first major cycle after a recoverable power transient on either channel during Start Preparation through Post Shutdown Standby for Flight or FRT-1 configuration, the in-control DCU shall perform the following:
  - (1) [IR136:5192;2] The five propellant valves on the in-control actuator channel shall be checked to verify that the actuator commands and positions agree within +/- 6% for Channel A or +/-10% for Channel B. [IR136:5192;3] This check shall be performed independent of component qualification. [IR136:5192;4] This check shall be bypassed for any of the following conditions:
    - (i) [IR136:5192;5] During Hydraulic Lockup (3.2.3:1.7.2).
    - (ii) [IR136:5192;6] During Pneumatic Shutdown (Table XIV).
    - (iii) [IR136:5192;7] During the Terminate Sequence mode of Post Shutdown when time is greater than or equal to 0.64 seconds (Table XV, Part A).



3.2.1:2.3 Major Cycle Restart (Continued)

- (2) [IR136:5192;8] The first propellant valve to exceed the +/- 6% limit on Channel A or the +/-10% limit on Channel B, shall cause the in-control actuator channel to be disqualified.
- (1) If control loops are active and, if Major Cycle Restart was entered due to PRI or cross-channel power interruption, then control loop computations will be bypassed in the first major cycle. Otherwise, normal control loop computations will be performed, as specified in Table XI.
- (m) [IR143:1394;1] Whenever a major cycle is interrupted and a Major Cycle Restart performed, the value of Time Reference shall remain the same as that in effect for the interrupted major cycle, unless a reset to zero was required prior to the interruption. [IR144:1394;1] If a reset to zero was required before the interruption, Time Reference shall be set to zero in the new major cycle.
- (n) [IR144:1843;1] The coming major cycle shall be initiated as a non-VDT transmitting cycle.
- (o) [IR144:4863;1] The in-control DCU shall update the OE On/Off Registers to reflect the corresponding engine state within the first major cycle, unless an OPOV travel check is to be performed. OPOV travel is checked when Major Cycle Restart is entered via Major Cycle Initiation After PRI, and an indication had been set to check for OPOV travel.

If OPOV travel check is to be performed:

- (1) [IR144:4863;2] In the first major cycle the OE On/Off Registers shall remain in the temporary configuration defined by (d) (2), unless hardware disqualification occurs.
- (2) [IR144:4863;3] In the second major cycle, OPOV position shall be verified to be partially open and not more than 3.4 percent of full scale from its last indicated position. This check will be performed per the following:

3.2.1:2.3 Major Cycle Restart (Continued)

- (i) [IR144:4863;4] Once the OE RVDT/RVDT Excitation Power Supply Self-Test (3.2.3:3.3.4) is performed in the second major cycle, if OPOV (RVDT) position data from at least one channel is qualified, and if the OPOV position is  $\geq$  6 percent open, and if the 3.4 percent limit is not exceeded, then the current phase and mode shall be retained.
- (ii) [IR144:4863;5] Otherwise, Pneumatic Shutdown of the engine shall be initiated as defined for PS response, 3.2.4:4 (w).
- (iii) [IR144:4863;6] In either case, the OE On/Off Registers shall be commanded to reflect the corresponding engine state within the second major cycle.
- (p) [IR144:4863;7] If both DCUs are operational and Major Cycle Restart was entered due to a power recovery on either channel, the OE On/Off Registers shall be updated to reflect the corresponding engine state within 94.5 msec from the onset of the power interruption.
- (q) Purge and Ancillary Systems Monitoring will be suspended in the coming major cycle.
- (r) [IR145:4702;1] Command Voting, 3.2.2:1.2, shall be performed unconditionally in the first major cycle at the normally scheduled time.

3.2.1:3 Watchdog Timer (WDT) Control

The WDTs provide a means of removing their DCU from control if it does not perform periodic resetting of the timers. This provides protection against computer failure, software Stops or loss of sequencing.

Control of the WDTs is based on the following:

- (a) Each WDT times-out 18 +3 msec after it is last reset. [IR154:3197;1] Each WDT shall be reset every other minor cycle (10 +/- 2 msec) except where designated otherwise by the following:
  - (1) PROM/RAM Program Entry, 3.2.1:1.
  - (2) In-Channel Power Failure Response, 3.2.1:1.5.
  - (3) Major Cycle Initiation/Restart, 3.2.1:2.2 and 3.2.1:2.3.
  - (4) Self-disqualification of DCU/CIE, 3.2.1:6.1.
  - (5) Fail-operational Channel Switchover portion of Actuator Checkout, 3.2.3:2.3.4.
  - (6) Controller Checkout Tests, 3.2.3:2.3.5.
  - (7) Igniter Checkout Test, 3.2.3:2.3.2.
- (b) [IR156] Logic to reset WDT1 shall be in low RAM and the logic to reset WDT2 shall be in high RAM. This is to enable detection of failure in the address jam bit mechanism.
- (c) WDT(s) will be reset in Major Cycle Initiation and in Major Cycle Restart.
- (d) [IR157:1386;1] The WDTs shall be reset after completion of the TRI response routine to protect from continuous TRIs that could continuously reset a WDT.

3.2.1:3 Watchdog Timer (WDT) Control (Continued)

(e) [IR157:1386;2] WDT2 shall be reset in minor cycles 1 and 3. [IR157:1386;3] WDT1 shall be reset in minor cycles 2 and 4.

(f) A WDT time-out is signaled by the corresponding interrupt, either WDT1 or WDT2. [IR160:1386;1] When a WDT1 or WDT2 occurs, the DCU/CIE shall be disqualified per 3.2.1:6.1. [IR161] These interrupts shall normally be maintained in an enabled state. Specific exceptions are during:

- (1) PROM/RAM Program Entry, 3.2.1:1.
- (2) Major Cycle Initiation/Restart, 3.2.1:2.2 and 3.2.1:2.3.
- (3) When other interrupts are disabled via an interrupt level while responding to another interrupt.
- (4) Controller Checkout Tests, 3.2.3:2.3.5.

3.2.1:4 Computer Status and Exception Control

[IR169:6261;1] Whenever the contents of a CIE interrupt mask register are to be modified, an image of the CIE interrupt mask register data shall be retained in RAM, except during Controller Checkout when the mechanics of CIE interrupt mask register manipulation may be defined by Design. An image of the CIE interrupt mask register data is retained in RAM for use by the Operational Program because data cannot be fetched from the CIE interrupt mask registers.

The Operational Program will return to the appropriate processing once it has responded to interruptions, exception processing, or temporary power losses which do not lead to DCU disqualification. This will be accomplished by adhering to the requirements specified in Exception Vector Handling, 3.3.4:6. In addition, the following safeguards will be taken in response to exception requests:

- (a) Reentrance to a routine in execution due to exceptions or monitoring functions will be controlled to ensure preservation of the original program linkage. To do this the following rules will be followed:

3.2.1:4 Computer Status and Exception Control (Continued)

(1) [IR170] When reentry can be caused by an interrupt, that interrupt shall be disabled (via the interrupt level) while the routine is being executed. This is allowable if the resulting interrupt response delay is within specification requirements.

(2) [IR171] If rule (1) cannot be followed, the reentrant routine shall have all linkages, and parameters passed on the appropriate stack (either supervisor or user) or in registers. [IR172] All data used in the routine shall then be maintained on the appropriate stack.

- (b) Some monitoring/checking or initialization functions require that an exception be generated (for example, in the DCU Exception Processing Test of 3.2.3:2.2.1). In such cases, if the exception request occurs, the response is part of the monitoring function and not the normal exception response.

An acceptable approach in identifying normal vs. monitor is to set an indication that such a monitoring task is in effect. That indication is examined at the beginning of the exception response sequence and the appropriate path is taken. If the monitoring path is taken, the indication is cleared and so verified before proceeding with the monitoring task. This prevents permanent disabling of the normal exception response.

- (c) When an interrupt is received, the corresponding interrupt response routine is entered. Upon entry, the Interrupt Decoder Self-Test (3.2.3:3.1.5) is performed which verifies that the interrupt is pending, and except for PFI and PRI, that it is enabled in the CIE. [IR173:6245;1] If the Interrupt Decoder Self-Test passes, an immediate retry shall be performed if the interrupt is an SCPI, WDT1, WDT2, RCFI1, RCFI2, or ADPFI. The immediate retry entails clearing the interrupt and rechecking the pending bit. [IR173:6245;2] If the interrupt is still pending, the interrupt response routine shall be completed; otherwise, a return shall be made to continue the normal processing of the Operational Program as the interrupt was only a transient.

### 3.2.1:4.1 Computer Exceptions

An exception is a general category of items which can interrupt the processing in a MC68000 microprocessor. Exceptions are categorized into four basic types:

- (a) MC68000-defined exceptions (for example, Reset, Bus Error, Zero Divide) which cannot be disabled by software.
- (b) User-defined interrupts, which in this document are referred to as Interrupts (for example, PFI, PRI, SEII).
- (c) Non-implemented Exceptions for Flight Controllers (for example, Stack Overflow/Underflow Interrupts used on the Brassboard).
- (d) Exceptions which are not implemented in either a Flight Controller or the Brassboard (for example, Line 1010 Emulator/Line 1011 Emulator which are assigned to vectors 10/11, but are designated as illegal vectors, see Table XL).

### 3.2.1:5 Exception Processing

[IR175] Once the Operational Program has started processing an interrupt, that interrupt shall be cleared before completing the interrupt routine. The processing required in response to each exception is described below.

#### 3.2.1:5.1 Reset Exception (PROM)

The function of the Reset Exception that vectors to a location in PROM is described in 3.1.3:2.1.1 and the PROM Spec.

#### 3.2.1:5.2 Reset Exception (RAM)

The Reset Exception vectors in RAM are unused and can be accessed only via a hardware failure. [IR192:3280;1] This exception shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.3 Bus Error Exception

[IR194:3280;1] If the Bus Error Exception is not the expected result of the DTACK Monitor/Bus Error Generator Test of 3.2.3:2.3.5:3, it shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.4 Address Error Exception

[IR196:3280;1] If the Address Error Exception is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.5 Illegal Instruction Exception

[IR198:3280;1] If the Illegal Instruction Exception is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.6 Zero Divide Exception

[IR199:3280;1] If the Zero Divide Exception is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.7 CHK Instruction Exception

This exception may be used at the discretion of the software designers. [IR200:3280;1] If the CHK Instruction Exception is not used by design or is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

3.2.1:5.8 TRAPV Instruction Exception

This exception may be used at the discretion of the software designers. [IR201:3280;1] If the TRAPV Instruction Exception is not used by design or is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

### 3.2.1:5.9 Privilege Violation Exception

[IR203:3280;1] If the Privilege Violation Exception is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1, it shall disqualify the DCU/CIE in which the exception occurred.

### 3.2.1:5.10 Trace Exception

This exception may be used at the discretion of the software designers. [IR204:3280;1] If the Trace Exception is not used by design, it shall disqualify the DCU/CIE in which the exception occurred.

### 3.2.1:5.11 Illegal Exception Vectors

Table XL defines the MC68000 exception processing vectors configured for the Block II SSMEC. All of the unused and reserved exception vectors are defined as illegal vectors. Two of these vectors (10 and 11) are tested in the DCU Exception Processing Test of 3.2.3:2.2.1. [IR205:3280;1] If either of these illegal vectors is not the expected result of the test of 3.2.3:2.2.1, or if any other illegal vector occurs, it shall disqualify the DCU/CIE in which the illegal exception occurred.

### 3.2.1:5.12 Spurious Interrupt Exception

The Spurious Interrupt Exception is activated when a bus error occurs during an interrupt acknowledge cycle or while fetching data from an interrupt vector location. [IR207:3280;1] This exception shall disqualify the DCU/CIE in which the exception occurred.

### 3.2.1:5.13 TRAP Instruction Exceptions

These exceptions may be used at the discretion of the software designers. [IR208:3280;1] If a TRAP Instruction Exception is not used by design, or is not the expected result of the DCU Exception Processing Test of 3.2.3:2.2.1 or the Failure Data Recorder Test of 3.2.3:2.3.5:28, it shall disqualify the DCU/CIE in which the exception occurred.

### 3.2.1:5.14 PFI

The requirements for this interrupt were previously described in 3.2.1:1.5.



3.2.1:5.15 PRI

The requirements for this interrupt were previously described in 3.2.1:1.6.

3.2.1:5.16 SCPI

[IR210:6245;1] If the SCPI is not a transient interrupt per 3.2.1:4(c), and is not the expected result of the SCP Interrupt Test of 3.2.3:2.3.5:2, it shall disqualify the DCU/CIE in which the interrupt occurred.

3.2.1:5.17 WDTH1 and WDTH2

[IR210:6245;2] If either a WDTH1 or WDTH2 is not a transient interrupt per 3.2.1:4(c), and is not the expected result of the Watchdog Timer Counter/Time Reference Test of 3.2.3:2.3.5:14 or the Watchdog Timer Interrupt Test of 3.2.3:2.3.5:15, or WDTH1 is not the expected result of the Failure Data Recorder Test of 3.2.3:2.3.5:28, the response to the interrupt shall be as defined in 3.2.1:3(f).

3.2.1:5.18 SEII

[IR210:1386;3] If an SEII is not the expected result of the Servoactuator Error Indication Interrupt Test of 3.2.3:2.3.5:26 or the OE Servoactuator Model/Monitor Self-Test of 3.2.3:3.2.4, the response to this interrupt shall be as defined in 3.2.3:6.1.

3.2.1:5.19 TRI

[IR210:1386;4] If the TRI is not the expected result of the Watchdog Timer Counter/Time Reference Test of 3.2.3:2.3.5:14 or the Failure Data Recorder Test of 3.2.3:2.3.5:28, the response to this interrupt shall be as defined in 3.2.1:2.1 and 3.2.1:2.3.

3.2.1:5.20 RCFI1 and RCFI2

[IR210:6245;3] If either RCFI1 or RCFI2 is not a transient interrupt per 3.2.1:4(c), and is not the expected result of the Watchdog Timer Counter/Time Reference Test of 3.2.3:2.3.5:14 or the Watchdog Timer Interrupt Test of 3.2.3:2.3.5:15, the responses to the interrupt shall be as defined in 3.2.1:2.2 and 3.2.1:9.

3.2.1:5.21 ADPFI

[IR210:6245;4] If the ADPFI is not a transient interrupt per 3.2.1:4(c), the responses to this interrupt shall be as defined in 3.2.1:2.2 and 3.2.1:9.

3.2.1:5.22 CIE Erroneous Acknowledge Level Interrupt

[IR211:3280;1] This interrupt shall disqualify the DCU/CIE in which the interrupt occurred.

3.2.1:5.23 Spurious CIE Interrupt

[IR212:3280;1] This interrupt shall disqualify the DCU/CIE in which the interrupt occurred.

3.2.1:6 Disqualifications of Controller Components

[IR212:4184;1] If an IE becomes temporarily disqualified (under strike), all IE DPM data from that IE shall be temporarily disqualified for the major cycle in which the error was detected. However, if the IE becomes permanently disqualified, selected IE DPM data will not be disqualified in order to perform OE and servoactuator tests, per 3.2.1:6.2(f). [IR212:4184;2] Temporarily or permanently disqualified data shall not be used for any purposes other than scaling and reporting in the VDT. [IR212:59;3] However, when a component in failing a monitoring test, becomes temporarily disqualified, the data used to qualify the component shall continue to be monitored for any ensuing failures.

If a controller component is already disqualified, any subsequent disqualification procedures for that component are to be bypassed unless stated otherwise.

[IR212:1843;1] All actions of the ensuing disqualification procedures shall be performed immediately.

For a simulated disqualification of a DCU or OE channel during FRT-1, refer to 3.2.3:2.4.3:1.

3.2.1:6.1 Self-disqualification of DCU/CIE

[IR212:2168;3] When it is necessary for a DCU to disqualify itself the following steps shall be performed in the following order:

- (a) [IR212:2979;1] All interrupts shall be disabled with the exception of PFI.
- (b) [IR213:3355;1] If the self-disqualification of the DCU/CIE results in a FID 75/76, the Failure Identification Word shall be generated per 3.2.4. If a second IE or OE channel failure was the cause of the DCU/CIE self-disqualification, the Failure Identification Word will have been generated as a result of the IE or OE disqualification.  
[IR213:3355;2] In all cases of self-disqualification, the failing DCU, if it becomes the in-control DCU, shall report the failure via a VRC transmission when the Operational Program restarts after exiting PROM.
- (c) [IR213:3997;1] If this is the first self-disqualification of the DCU/CIE subsequent to either an exit from PROM, via an Exit PROM command, or acceptance of a Controller Reset command, then the Central Processing Unit (CPU) Stop Status shall be recorded in RAM Main Memory. [IR213:1386;2] This Status shall be composed of the appropriate FID and the contents of the CPU's program counter, status register, and all address and data registers.
- (d) [IR213:1386;3] A Terminate IE Sequence I/O instruction shall be executed.
- (e) [IR213:594;5] Power to both OEs shall be turned off via the OE Power Control Switch.
- (f) [IR213:4236;1] If DCU B is in control, then it shall issue a Set +5V Under Voltage Test I/O instruction. In response to this I/O instruction, hardware will time-out WDT2 and generate a clear signal to OE B's On/Off Registers, resulting in an effective pneumatic shutdown of the engine. This sequence thus provides a fail-safe protection against both DCU A's WDTs failing into the non-timed out state.

3.2.1:6.1 Self-disqualification of DCU/CIE (Continued)

- (g) [IR213:594;6] Fast time-out of both WDTs shall be performed.
- (h) [IR213:4934;1] If disqualification is due to Assured Pneumatic Shutdown monitoring, the DCU shall perform the following in the given order:
  - (1) Issue a Set +5V Under Voltage Test I/O instruction.
  - (2) Delay for at least 2 usec.
  - (3) Issue a Reset +5V Under Voltage Test I/O instruction.
- (i) [IR213:1386;5] An MC68000 STOP instruction shall be executed.
- (j) [IR213:1386;6] Following the STOP instruction shall be an MC68000 BRA instruction whose displacement field specifies that the next instruction to be executed is the aforementioned STOP instruction.

3.2.1:6.2 Disqualification of an IE Channel

[IR214:591;1] A failure of either IE Channel A or B shall result in the following responses for the respective IE channel:

- (a) [IR214:2979;1] TRI, RCFI1, RCFI2, and ADPFI shall be disabled. SEII monitoring will be suspended (3.2.3:6.1.3).
- (b) [IR214:4184;1] The following tests shall be suspended on the disqualified IE channel:
  - (1) 3.2.3:3.3.1, IE Address and Data Bus Self-Test
  - (2) 3.2.3:3.3.3, IE Analog to Digital Converter Self-Test
  - (3) 3.2.3:3.3.6, PSE Internal Voltages Self-Test
  - (4) 3.2.3:3.3.7, IE (VSPE) Channel C Power Supply Self-Test

3.2.1:6.2 Disqualification of an IE Channel (Continued)

- (5) 3.2.3:2.2.2, PSE Output Voltages Maintenance Monitoring Test
- (c) [IR214:4184;2] The following selected sensors shall be disqualified:
  - (1) accelerometers
  - (2) temperatures
  - (3) pressures
  - (4) flowrates
  - (5) shaft speeds
  - (6) Pogo RIV
  - (7) LVDTs

The frequency and amplitude for the 2khz excitation, RVDT position data, and LDA input data will not be disqualified so that the data will be available for the OE and servoactuator tests.

As the final response, a Major Cycle Restart will be performed.

- (d) When the cross-channel IE and DCU are being disqualified due to a power loss, Major Cycle Restart will be performed after the cross-channel DCU disqualification.
- (e) [IR214:4184;3] In all other cases, Major Cycle Restart shall be performed immediately.

After the IE is disqualified:

- (f) [IR214:5546;1] For a qualified OE and servoactuator channel, those tests that monitor the OE and servoactuators by testing IE DPM data shall continue to use the data from a disqualified IE. These tests are:
  - (1) 3.2.3:3.3.2:1, Pulse Rate Converter Self-Tests, 2khz RVDT/LVDT Excitation Frequency

3.2.1:6.2 Disqualification of an IE Channel (Continued)

- (2) 3.2.3:3.3.4, OE RVDT/LVDT Excitation Power Supply Self-Test
- (3) 3.2.3:3.3.5, OE Digital to Analog Converters Self-Test
- (4) 3.2.3:6.1.4, RVDT Comparison Test
- (5) 3.2.3:6.1.7, Actuator Settling Check

3.2.1:6.3 Disqualification of an OE Channel

[IR215:591;1] A failure of either OE Channel A or B shall result in the following responses for the respective OE channel:

- (a) [IR215:2979;1] TRI, RCFI1, RCFI2, and ADPFI shall be disabled. SEII monitoring will be suspended (3.2.3:6.1.3).
- (b) [IR215:3235;1] The OE self-tests shall be suspended.

Sections (c) through (i) below will be accomplished by loading the storage registers and transferring the contents. If the OE is disqualified because of an OE Storage Register failure, no loading or transferring of this Storage Register will be performed per 3.2.3:3.1.7. The OE Storage Registers Self-Test and Engine/Controller On/Off Devices Self-Test will not be performed.

- (c) [IR215:1386;1] All solenoids shall be deenergized.
- (d) [IR215:1386;2] All fail-safe servoswitches shall be deenergized.
- (e) [IR215:591;5] All igniters shall be deenergized.
- (f) [IR215:3704;1] Group 1 (Sensor Checkout) and Group 2 (Propellant Drop Sensor) switches shall be deactivated in both OE channels.
- (g) [IR215:1386;4] The PRC Overflow Test shall be deactivated.
- (h) Halt Exit will remain disabled.

3.2.1:6.3 Disqualification of an OE Channel (Continued)

- (i) [IR215:1386;5] If the source of RVDT/LVDT excitation is to be switched to CIE B during the ensuing disqualification of the servoactuators, the OE A Power Control Switch shall be commanded off after 20 +/- 10 msec to allow the fail-operational switches to take effect. [IR215:3528;1] Else the source of excitation will be retained, and the OE Power Control Switch shall be commanded off immediately subsequent to the suspension of SEII monitoring in 3.2.3:6.1.3.
- (j) [IR215:1386;7] There shall be no commands transmitted to a disqualified OE channel except for:
  - (1) Commanding the OE Power Control Switch off each major cycle.
  - (2) Updating the OE Power Control Switch and the OE On/Off Registers in Major Cycle Restart, 3.2.1:2.3(d) (1).
- (k) [IR215:3528;2] As the final response, the servoactuators on the respective OE channel shall be disqualified, unless previously disqualified.

The delimiters in Table I will designate whether an IE failure occurred prior to an OE failure.

3.2.1:6.4 Disqualification of Servoactuators

[IR216:2979;1] The failure of one or more servoactuators on the same channel shall result in the disqualification of all the servoactuators and the RVDT data on that channel.

[IR216:3235;1] Upon disqualification of any servoactuator channel, TRI, RCFI1, RCFI2, and ADPFI shall be disabled.

[IR216:3235;2] The OE Digital to Analog Converters Self-Test of 3.2.3:3.3.5 shall be suspended for the servoactuator channel being disqualified. SEII monitoring will also be suspended (3.2.3:6.1.3).

Channel-dependent servoactuator disqualification requirements are as follows:

3.2.1:6.4 Disqualification of Servoactuators (Continued)

- (a) For servoactuator failures on Channel A, where Channel B servoactuators are qualified, and the RVDT miscompare cases of 3.2.3:6.1.4 (b) and (c) do not pertain:
- (1) [IR216:2979;4] Control shall be switched to Channel B servoactuators by energizing all fail-operational servoswitches.
  - (2) [IR216:591;3] The source of RVDT/LVDT excitation shall be switched to CIE B. Both OEs will continue to receive excitation after the source has been switched.
- (b) For servoactuator failures on Channel A during Start or Mainstage, where Channel B servoactuators are qualified, and there had been a prior RVDT miscompare (3.2.3:6.1.4 (b) and (c)), only the Channel A servoactuators will be disqualified, and the following performed:
- (1) [IR216:2979;5] The OE Digital to Analog Converters Self-Test of 3.2.3:3.3.5 shall be suspended for servoactuators on Channel B.
  - (2) [IR216:2979;6] The source of RVDT/LVDT excitation shall be switched to CIE B. Both OEs will continue to receive excitation after the source has been switched.
- If this condition occurs while in Mainstage, Hydraulic Lockup will be declared. As a result of Hydraulic Lockup, Channel B servoactuators will be considered to be disqualified.
- (c) For servoactuator failures on Channel B, where Channel A servoactuators are qualified, the aforementioned general disqualification requirements are sufficient.
- (d) For simultaneous servoactuator failures on both Channels A and B, the aforementioned general requirements apply to both channels.

Subsequent to any servoactuator disqualification, a Major Cycle Restart will be performed.



3.2.1:6.4 Disqualification of Servoactuators (Continued)

- (e) When the cross-channel servoactuator channel and DCU are being disqualified due to a power loss, Major Cycle Restart will be performed subsequent to the cross-channel DCU disqualification.
- (f) [IR216:3235;3] In all other cases, Major Cycle Restart shall be performed immediately.

3.2.1:6.5 Disqualification of the Cross-Channel DCU/IE/OE

[IR216:1208;1] When it is necessary for a DCU to disqualify the cross-channel DCU, the following requirements shall pertain.

- (a) [IR216:2092;1] TRI and RCFIs shall be disabled.
- (b) SEII monitoring will be suspended (3.2.3:6.1.3).
- (c) [IR216:2092;2] The appropriate OE On/Off Register bit shall be set immediately to indicate Power Off Time in the cross-channel has been exceeded.  
[IR216:3235;4] The OE Storage Registers Self-Test, 3.2.3:3.1.7, shall be suspended for this update. The cross-channel Power Off Time Exceeded indication will be set by loading the storage registers and transferring the contents. [IR216:3235;5] The Engine/Controller On/Off Devices Self-Test, 3.2.3:3.2.3, shall be performed. This guarantees DCU self-disqualification if the OE cannot be updated to indicate cross-channel Power Off Time Exceeded.
- (d) [IR216:4184;1] If either PBD or ADPFI indicates cross-channel power failure, the cross-channel IE shall be disqualified, per 3.2.1:6.2, and the cross-channel OE and servoactuators shall be disqualified per 3.2.1:6.3. A Major Cycle Restart due to the disqualifications of the IE and OE will be performed after the cross-channel DCU disqualification, except for DCU B takeover.
- (e) [IR216:2092;3] ADPFI shall be disabled.
- (f) [IR216:2092;4] If the in-channel is DCU B, then DCU B Takeover Immediate Functions shall be executed, per 3.2.1:9.1.1.

### 3.2.1:7 Fault Traceability Provisions

It is important to provide a degree of fault traceability that isolates the self-test or monitoring function that caused removal of the DCU from operation. This is provided by:

- (a) The CPU Stop Status saved per 3.2.1:6.1.
- (b) The FDR, which is inhibited from further recording by hardware.

In addition, the user/supervisor stacks provide a record of the program step initiating the linkage to the above sequences. The record is not needed as a return address but is used for traceability.

With the described provisions of the Operational Program, identification of the fault-detecting function will be possible from examination of the following data:

- (c) Failure Identification Word,
- (d) User/supervisor stacks,
- (e) Recorded state of the CPU's registers,
- (f) Contents of the Failure Data Recorder.

This data will provide adequate traceability, even if the disqualification occurs while interrupts are enabled. This information may be accessed using the PROM without cycling the Operational Program; however, the PROM will redefine and use the supervisor stack.

To assure meaningful contents in the trace locations, the Operational Program will clear the CPU Stop Status as part of Controller Reset processing, 3.2.3:1.1.1.

### 3.2.1:8 Standby DCU Processing

The standby DCU maintains itself in a state of readiness to assume control if the in-control DCU fails. This is accomplished by tracking the relevant phase/mode changes, controller electronics, control loop functions, and by monitoring the relevant sensor functions. The standby DCU will disqualify itself if it finds itself not ready to assume control. The standby DCU will perform the appropriate DCU self-testing and monitoring of accessible CIE functions per Controller Continual Self-Tests of 3.2.3:3.

#### 3.2.1:8.1 Configuration/Phase/Mode Tracking

Tracking of the in-control DCU by the standby DCU is performed to:

- (a) Ensure that a takeover by the standby DCU will occur safely, and that the memory configuration and engine phase/mode existing prior to failure of the in-control DCU, will be maintained.
- (b) Provide additional command implementation criteria for selected commands. This is to ensure that the standby DCU can track the in-control DCU, and to detect VEEI command channel failures in the standby DCU.
- (c) Afford the standby DCU the ability to follow the in-control DCU through the relevant commanded and non-commanded configuration/phase/mode changes.
- (d) Allow communication between DCUs for checkout sequences requiring handshaking. Checkout sequences relevant to the standby DCU are Sensor Checkout and Controller Checkout, see 3.2.1:8.2.
- (e) Minimize engine transients at takeover due to failure of hardware components.

Tracking of memory configuration and engine phase/mode is handled in this paragraph. Other tracking requirements are described in 3.2.1:8.2 and 3.2.1:8.3.

The standby DCU will change its configuration/phase/mode based upon command acceptance, detected configuration/phase/mode, or command acceptance substantiated by the detected configuration/phase/mode.

3.2.1:8.1 Configuration/Phase/Mode Tracking (Continued)

The detected configuration/phase/mode state represents the configuration/phase/mode of the in-control DCU as observed by the standby DCU. [IR221:1789;1] The standby DCU shall detect the in-control DCU's configuration/phase/mode by examining the validated Engine Data Word (EDW) obtained per 3.2.3:3.1.2:3.

For commands that must be substantiated, a worst case time is defined at which the commands and detected configuration/phase/mode should agree. This time is called the IDSR/command cutoff point. [IR221:3300;1] This cutoff shall occur within the major cycle subsequent to detection of the associated configuration/phase/mode change.

The tracking requirements are as follows:

(f) Response to VEEI commands by the standby DCU will be as follows:

(1) [IR222:2840;1] Command voting shall be performed per 3.2.2:1.2. [IR222:2840;2] An exception is that the Start and Start Enable commands shall require only a 2 of 3 vote.

(2) [IR222:2840;3] Command acceptance and implementation shall be performed per 3.2.2:1.3 with the following conditions:

(i) [IR222:3605;1] Accepted Memory Readout B commands shall be implemented by DCU B per 3.2.2:2.1.2, if and only if the validated Engine Data Word indicates DCU B is the source of VRC data within 85 msec of acceptance of the Starting Address command.

(ii) [IR222:500206;1] Accepted IO Readout B commands shall be implemented by DCU B per 3.2.2:2.1.2, if and only if the validated Engine Data Word indicates DCU B is the source of VRC data within 85 msec of acceptance of the readout command.

(iii) [IR223:3300;1] Accepted Enter Ground Checkout, Enter FRT-1, Enter FRT-2, Enter Flight, Purge Sequence 1, 2, 3, 4, Start Enable and Start commands received by the standby DCU shall not be implemented unless the in-control DCU has initiated the command. The initiation of the command is confirmed by detecting the appropriate configuration/phase/mode change in the validated Engine Data Word, (see item (h) (2)).

3.2.1:8.1 Configuration/Phase/Mode Tracking (Continued)

- (iv) [IR223:2840;5] When an accepted Start command is substantiated by detection of the Start phase in the in-control DCU, the standby DCU shall delay 5 msec, perform a Major Cycle Restart (as defined in 3.2.1:2.3), and initiate the Start phase. This requirement is imposed so that the standby DCU will follow the in-control DCU into Start, but with a delay of 10 to 30 msec.
  - (v) [IR224:2419;1] An accepted Terminate Sequence or Deactivate All Valves command shall not be implemented.
  - (vi) [IR225:1789;1] An accepted Restore VRC command shall be implemented per 3.2.2:2.2.4. [IR225:1789;2] An accepted Controller Reset command shall be implemented per 3.2.3:1.1.1.
  - (vii) [IR226:1439;1] All other accepted commands (except the Component Checkout commands, see 3.2.1:8.2) shall be executed as if normally commanded when the DCU is in control.
- (g) General responses to the IDSR by the standby DCU are as follows:
- (1) [IR227:1439;1] The timing within the major cycle at which the IDSR is interrogated by standby DCU, shall be selected such that detection of a new Engine Data Word configuration always occurs after the corresponding VEEI command voting has taken place. Interrogation of the IDSR will be performed as specified in 3.2.1:2.1.1.
  - (2) [IR227:3300;1] The validated Engine Data Word shall be examined at least once per major cycle to detect the configuration/phase/mode (excluding PROM) of the in-control DCU.
  - (3) [IR228:4184;1] Data transmitted between the DCUs via the IDSR shall be as specified by Table XLII.
  - (4) [IR229:1789;1] If the data in the validated Engine Data Word matches one of the bit codes specified in Table XLII, the tracking logic of item (h) shall be executed.

3.2.1:8.1 Configuration/Phase/Mode Tracking (Continued)

[IR230:1439;1] If no match is found for four consecutive major cycles and the current phase is Start Preparation, the standby DCU shall be disqualified (per 3.2.1:6.1); else, no action shall be taken.

(h) The standby DCU's response (or tracking logic) to changes in the detected configuration/phase/mode is as follows:

(1) [IR231:3300;1] If the detected configuration/phase/mode is the same as the current configuration/phase/mode of the standby DCU, no change shall be made.

(2) [IR232:3300;1] Else, if all the following are true, then Enter Ground Checkout, Enter FRT-1, Enter FRT-2, Enter Flight, Purge Sequence 1, 2, 3, 4, Start Enable, or Start is commanded and substantiated, and that command shall be initiated by the standby DCU:

(i) [IR232:3300;2] The new configuration is Ground Checkout, FRT-1, FRT-2, Flight or the new detected phase/mode is Purge Sequence 1, 2, 3, 4, Start Enable, or Start.

(ii) [IR232:3300;3] The detected configuration/phase/mode corresponds to either of the last two commands accepted by that DCU (see (f) (2) (iii)).

(iii) [IR232:3494;1] The corresponding command is received prior to the IDSR/command cutoff point.

(3) Else, the detected configuration/phase/mode represents an action by the in-control DCU which is not expected by the standby DCU; the response will be as follows:

(i) [IR234:1439;1] If the detected phase/mode represents Checkout Standby and the current phase is Checkout then the standby DCU shall enter Checkout Standby.

3.2.1:8.1 Configuration/Phase/Mode/Tracking (Continued)

- (ii) [IR234:3300;1] If the detected configuration represents a transition into Ground Checkout, FRT-1, FRT-2, or Flight for which no command has been accepted, prior to the IDSR/command cutoff point, the standby DCU shall disqualify itself.
- (iii) [IR235:3494;1] With the exception of the conditions described in items (iv) and (v) below, if the detected phase/mode represents a transition into Purge Sequence 1, 2, 3, 4, or Start Enable for which no accepted command has been received, prior to the IDSR/command cutoff point, the standby DCU shall disqualify itself.
- (iv) [IR235:2840;2] If the detected phase/mode represents Purge Sequence 3 and the current engine state is Purge Sequence 4, Engine Ready, or Start Enable, then the standby DCU shall enter Purge Sequence 3.
- (v) [IR235:2840;3] If the detected phase/mode represents Purge Sequence 4 and the current engine state is Engine Ready or Start Enable, then the standby DCU shall revert to Purge Sequence 4 using the sequence of Table X, Part H (Purge Sequence 4 Rollback).
- (vi) [IR235:1439;5] If the detected phase/mode represents Engine Ready and the current phase/mode is Purge Sequence 4, then the standby DCU shall enter Engine Ready.
- (vii) [IR236:3494;1] If the detected phase/mode represents Start and no Start command has been accepted prior to the IDSR/command cutoff point, the standby DCU shall disqualify itself.
- (viii) [IR237:1439;1] If the detected phase/mode represents any of the stages of ignition confirmation and the current phase is Start, then the standby DCU shall enter the detected ignition confirmation stage.

3.2.1:8.1 Configuration/Phase/Mode Tracking (Continued)

- (ix) [IR237:1713;1] If the detected phase/mode represents Electrical Lockup, the standby DCU shall enter the Electrical Lockup mode and issue a non-resumable Major Component Failed (MCF).
- (x) [IR237:2049;1] If the detected phase/mode represents Hydraulic Lockup, the standby DCU shall enter the Hydraulic Lockup mode, assume that Channel A and B servoactuators are disqualified and issue a non-resumable Major Component Failed.
- (xi) [IR238:2840;1] If the detected phase/mode represents non-commanded hydraulic shutdown (Throttling to Zero Thrust mode), and the current phase is Start or Mainstage, the standby DCU shall initiate Hydraulic Shutdown.
- (xii) [IR239:4187;1] If the detected phase/mode represents a non-commanded Pneumatic Shutdown mode, and the current phase is not Post Shutdown Standby, the standby DCU shall initiate Pneumatic Shutdown.
- (xiii) [IR239:2840;2] If the detected phase/mode represents a Terminate Sequence mode, the standby DCU shall initiate a Terminate Sequence mode as defined in Table XV, Part A.
- (xiv) [IR241:1439;2] Non-commanded engine phase/mode changes not specifically mentioned shall not be tracked by the standby DCU.

This logic and the CIE IDSR Self-Test provides protection against failures of DCU A affecting DCU B and against failures of signals to DCU B. It also protects against transients in DCU signals and skew in updating the IDSRs.

- (i) The tracking requirements assume the phase/mode sequencing capabilities shown in Figures 2 - 6 (normal and optional) only.
- (j) Other combinations allowed by the acceptance logic defined under 3.2.2, but not operationally allowable (not meaningful) may result in extraneous removal of DCU B from operation, but no unsafe response will be allowed.



### 3.2.1:8.2 Component Checkout Mode Tracking

When the standby DCU is in the Ground Checkout configuration, Component Checkout commands will be executed as follows:

- (a) [IR242] The Sensor Checkout And Calibration command shall be executed at least to the extent necessary to compute the sensor calibration coefficients. Coordination with the in-control DCU is necessary to obtain the correct ambient and simulated operation readings. [IR243] This coordination shall accommodate skew between the two DCUs in major cycle timing and in recognition of VEEI Commands.

DCU B may, if necessary, utilize the indicated state of the Sensor Checkout Switches to effect tracking/coordination with DCU A.

- (b) [IR244:1386;1] The Controller Checkout command shall be fully executed by the standby DCU per requirements of 3.2.3:2.3.5, Controller Checkout Tests.
- (c) [IR246:3300;1] All other Component Checkout commands shall be ignored by the standby DCU which will remain in the Checkout Standby mode.

### 3.2.1:8.3 OE A and Servoactuator Tracking

[IR247:4184;1] The standby DCU shall retain OE A, Channel A and B servoactuators, and RVDT miscompare status provided by the in-control DCU via the IDSR, and obtained from the validated Engine Data Word, per 3.2.3:3.1.2:3. This status is retained for the standby DCU to perform control loop tracking (3.2.1:8.4).

If the standby DCU detects that the in-control DCU has placed the engine in Hydraulic Lockup, the standby DCU will assume that Channel A and B servoactuators are disqualified.

### 3.2.1:8.4 Control Loop Tracking

[IR257] The standby DCU shall track the control loops to the extent necessary for proper initialization at takeover. This discussion includes control loops for all the propellant valves; although, the MCC Pc control loop is the major element of tracking.

#### 3.2.1:8.4 Control Loop Tracking (Continued)

[IR258:2076;1] During the Start phase, the standby DCU shall keep a record of the instantaneous values of all ramps for Pc Reference, cross-feed signals (the outputs from the MCC Pc control loop into the Mixture Ratio loop), and the Start schedule of individual propellant valves. [IR259] These shall be derived from computations identical to those of the in-control DCU. [IR260] Time Reference from Start shall be maintained counting from initiation of the Start phase as defined in 3.2.1:8.1.

[IR261] At the transition from Start to Mainstage (as indicated by its Time Reference), the standby DCU shall reinitialize its control loop integrators to accommodate a variable crossfeed gain. The requirement of variable crossfeed gain may be satisfied by reinitializing the MCC Pc control loop integrator only. [IR262:3074;1] It shall use the same equations and input parameters as used by the in-control DCU (reference step 45 of Table XI). [IR263:1394;1] In this reinitialization the standby DCU shall issue the OPOV and FPOV commands as indicated by the D/A output that is read via the IE. [IR264:1394;1] The current qualification status (3.2.1:8.3) shall be used in selecting the applicable servoactuators.

During Mainstage phase, there is no control loop tracking requirement beyond updating the Pc Reference. Shutdown phase processing is immediately initiated in DCU B upon command, as defined in 3.2.1:8.1.

#### 3.2.1:8.5 Standby DCU Sensor Monitoring

[IR272:1608;1] Qualification of sensor channel data shall be as defined in 3.2.3:4, but will affect the current major cycle only; i.e., no permanent disqualification.

#### 3.2.1:8.6 Standby DCU Monitoring for Ignition Confirmation

The standby DCU will be notified through the IDSR when any of the tests of ignition confirmation specified in 3.2.3:5.2 (a through c) pass (see 3.2.1:8.1(h) (3) (viii)). If a DCU B takeover occurs, this information will be used by DCU B to determine which tests of ignition confirmation must still be performed. The IDSR ignition confirmation data will be used in the eventuality of DCU switchover.

3.2.1:8.7 Standby DCU I/O Operations and Restrictions

I/O Operations and restrictions exist for the standby DCU to ensure fail-operational and fail-safe performance of the controller. The standby DCU:

- (a) [IR284:2000;1] Shall issue the Turn Off OE A/B Power Control Switch I/O instructions once per major cycle. These instructions attempt to turn off 2 khz excitation, solenoid, servoswitch, and igniter power supplies in both OEs.
- (b) [IR284:4457;1] Shall not issue the following OE I/O instructions unless in the process of cross-channel DCU disqualification:
  - (1) Load OE A/B Storage Register
  - (2) Transfer OE A/B Storage Register
  - (3) Turn On OE A/B Power Control Switch
- (c) [IR284:4457;2] Shall not issue the following IE I/O instructions unless in the process of self-disqualification:
  - (1) Initiate IE Operation
  - (2) Terminate IE Sequence
- (d) [IR284:500206;1] Shall not issue an Initiate VRC Data Transmission I/O instruction, except as required in response to a Switch VRC command (per 3.2.2:2.2.4) or in response to a Memory Readout B or IO Readout B command (per 3.2.2:2.1.2).

3.2.1:9 Cross-Channel DCU Failure and Power Loss Monitoring

This function comprises the monitoring and response to failures of the cross-channel's DCU/CIE and PSE. Information is available to the Operational Program in a DCU about the operational status of the cross-channel via four primary signals:

- o RCFI1 and RCFI2,
- o ADPFI,
- o Cross-Channel Power Bus Down (PBD) status.

Because of the specified procedure for PFI (per 3.2.1:1.5) and self-disqualification of a DCU (per 3.2.1:6.1), the two RCFIs will occur for either a DCU failure or power loss. To determine the appropriate response, ADPFI and PBD are examined.

3.2.1:9 Cross-Channel DCU Failure and Power Loss Monitoring  
(Continued)

ADPFI and PBD are also monitored to detect power loss following a DCU failure without power loss (to determine if the IE, OE on that channel has power).

The requirements for the individual cases are described in this paragraph.

[IR286:1208;1] Upon receipt of an RCFI1 or RCFI2, the in-channel DCU shall disable RCFIs. [IR286:1208;2] The ADPFI in the CIE shall be cleared, enabled, and the pending status examined.

[IR286:1208;3] If there is a cross-channel power loss, as determined by the existence of an ADPFI pending indication or PBD status, the functions of Power Interruption/Loss in Cross-Channel shall be performed, per 3.2.1:9.3.

Else, cross-channel power is within limits (but the DCU has failed), then,

- (a) [IR286:1208;4] The cross-channel DCU shall be disqualified, per 3.2.1:6.5.
- (b) [IR286:1208;5] Major Cycle Restart shall be performed, per 3.2.1:2.3.
- (c) In Major Cycle Restart, ADPFI will be enabled, permitting receipt of new interrupts for monitoring of cross-channel power loss.

3.2.1:9.1 DCU B Takeover

Whenever DCU A is disqualified, per 3.2.1:6.5, the procedure for DCU B Takeover will proceed in three phases, according to (a), (b), (c) below.

- (a) DCU B Takeover Immediate Functions will be executed, per 3.2.1:9.1.1.
- (b) Major Cycle Restart will be invoked.
- (c) DCU B Takeover Major Cycle Functions will be performed per 3.2.1:9.1.2.

3.2.1:9.1.1 DCU B Takeover Immediate Functions

IE A, IE B, and OE B will not be disqualified upon DCU B takeover because of a prior disqualification by DCU A. If servoactuator control was switched to Channel B prior to DCU B takeover, it will remain on Channel B after DCU B takeover.

[IR286:3280;1] When DCU A is disqualified, DCU B shall become the in-control DCU and the following functions shall be executed prior to Major Cycle Restart. If any of the functions below result in a failure which invokes Major Cycle Restart, the steps of the disqualification procedure will be followed, with the exception of Major Cycle Restart. This will be executed in step (c) below.

- (a) The disqualifications of any components as provided by the IDSR while DCU B was in standby will be retained per 3.2.1:8.3.
- (b) [IR292:4184;1] An OE Power Control Switch I/O instruction shall be issued to turn on the power supplies in all qualified OEs prior to loading of the OE On/Off Registers. [IR292:4184;2] For all qualified OEs, the OE On/Off Registers shall be initialized to the following temporary conditions:
  - (1) [IR292:4641;1] All solenoids shall be deenergized with the exception of the Emergency Shutdown Solenoid and the HPOP IMSL Purge Solenoid. [IR292:4641;2] The Emergency Shutdown Solenoid and the HPOP IMSL Purge Solenoid shall be commanded to reflect phase/mode and qualification status.
  - (2) [IR292:1394;4] All igniters shall be deenergized.
  - (3) [IR292:1394;5] Group 1 (Sensor Checkout) and Group 2 (Propellant Drop Sensor) switches shall be deactivated.
  - (4) [IR292:1394;6] The PRC Overflow Test shall be deactivated.
  - (5) The appropriate OE On/Off Register bit will be set to indicate Channel A Power-Off Time Exceeded.
  - (6) [IR292:1899;1] Halt Exit for DCU A and for DCU B shall be disabled.
  - (7) Servoswitches and RVDT/LVDT excitation will be maintained in accordance with 3.2.1:6.3 and 3.2.1:6.4. [IR292:4221;1] However, if the mode was Hydraulic Lockup at the time of DCU B takeover, the fail-operational servoswitches shall be energized.

3.2.1:9.1.1 DCU B Takeover Immediate Functions (Continued)

- (c) The functions of Major Cycle Restart, 3.2.1:2.3, will be performed.
- (d) [IR292:1208;1] Subsequent to Major Cycle Restart, DCU B Takeover Major Cycle Functions (3.2.1:9.1.2) shall be performed.

3.2.1:9.1.2 DCU B Takeover Major Cycle Functions

The following functions will be executed subsequent to Major Cycle Restart during DCU B Takeover.

- (a) [IR292:2049;1] The phase and mode as obtained from the tracking of 3.2.1:8.1, shall be implemented in the first major cycle.  

[IR292:429;12] If takeover occurs during any mode of Checkout, engine mode shall be set to Checkout Standby.
- (b) [IR292:754;1] In the first major cycle, data in the OE On/Off Registers shall be updated to reflect the qualification status of output devices. OE On/Off Register updates in subsequent major cycles will reflect the current phase/mode output device configuration as normally computed.
- (c) [IR292:4184;3] In the second and subsequent major cycles, a test shall be performed by clearing and enabling RCFI1 and RCFI2 once per major cycle to verify that both RCFIs are present. [IR292:4184;4] If either is absent for this single strike test, OE A shall be disqualified per 3.2.1:6.3.
- (d) [IR292:1386;2] If a Switch VRC to DCU B I/O instruction is in effect at the time of takeover, DCU B shall control the VRC as the in-control DCU, thus eliminating the processing defined in 3.2.2:2.2.4.
- (e) Upon takeover in Start, DCU B will use the validated Engine Data Word, obtained per 3.2.3:3.1.2:3 to determine what portion of Ignition Confirmation has been completed by DCU A. DCU B will then perform the Ignition Confirmation Tests not completed by DCU A at their scheduled times.
- (f) See 3.2.3:6.1.3 for SEII monitoring considerations.

3.2.1:9.2 Failure of DCU B

Whenever DCU B is disqualified, per 3.2.1:6.5, Major Cycle Restart will be performed.

3.2.1:9.3 Power Interruption/Loss in Cross-Channel

Upon receipt of RCFI1 or RCFI2, the in-channel DCU/CIE detects power loss in the cross-channel by receipt of an ADPFI indication, or by power down status in the PBD.

[IR300:1208;1] Power interruption or loss in the cross-channel while engine phase is Checkout, shall result in disqualification of the cross-channel DCU, IE, OE, and DCU B Takeover, if applicable, per 3.2.1:6.5. [IR300:1208;2] Major Cycle Restart shall then be performed per 3.2.1:2.3.

Power interruption or loss in the cross-channel while its DCU is operational and the engine phase is not Checkout, will cause the surviving DCU to allow for a 30 msec interruption of AC power plus 25 msec for PSE recovery before disqualifying the components on the unpowered channel. Allowing for a 30 msec AC power interruption and for a 25 msec PSE recovery, the surviving DCU waits 59.5 msec for power recovery in the cross-channel. This results in a maximum time of 94.5 msec from loss of AC power, to energizing of the appropriate servoswitches and solenoids. However, the commanded state of the Emergency Shutdown Solenoid and the HPOP IMSL Purge Solenoid will remain unchanged, independent of the power transient. During this 94.5 msec time interval, the OPOV valve travel should not deviate from its previously observed position by more than 3.4% of full scale actuator range.

Power loss in a channel after disqualification of its DCU will result in immediate disqualification of the corresponding IE and OE, unless previously disqualified.

3.2.1:9.3.1 Allowance for Power Interruption in the Cross-Channel

This function is required when power of the cross-channel is lost without a prior loss of the cross-channel DCU and engine phase is not Checkout. The Operational Program of the surviving DCU will perform the following:

- (a) [IR308] The contents of RTC shall be recorded to establish the time to next TRI.
- (b) [IR309:1899;1] If the in-channel OE is qualified,
  - (1) [IR309:1899;2] The in-channel DCU shall become the in-control DCU.

3.2.1:9.3.1 Allowance for Power Interruption in the Cross-Channel (Continued)

- (2) [IR309:4641;1] The power supplies and OE On/Off Registers shall be commanded, without performance of OE self-tests, to the following temporary configuration in the following order:
- (i) 2 khz excitation, solenoid, servoswitch and igniter power supplies turned on by using the Turn On in-channel OE Power Control Switch I/O instruction.
  - (ii) All in-channel solenoids, servoswitches and igniters deenergized, except the Emergency Shutdown Solenoid and the HPOP IMSL Purge Solenoid which remain unchanged. Leaving the Emergency Shutdown Solenoid energized would prevent a backdoor purge from extinguishing preburner ignition early in Start. Leaving the HPOP IMSL Purge Solenoid energized would maintain IMSL purge during power interruption/recovery.
  - (iii) RVDT/LVDT 2 khz excitation source selected.
  - (iv) The appropriate OE bit set to Cross-Channel Power Off Time not Exceeded.
  - (v) OE Power Control supplies turned off in the cross-channel by using the Turn Off cross-channel OE Power Control Switch I/O instruction each major cycle.
- (c) [IR310:1899;1] The in-channel DCU shall become the standby DCU.
- (d) [IR314] The functions of Major Cycle Restart, 3.2.1:2.3, shall be executed.
- (e) [IR315:1899;1] Subsequent to Major Cycle Restart, until either the cross-channel DCU/IE/OE is disqualified, or until power recovers within the allowed period specified in 3.2.1:9.3.1 (f), the surviving DCU shall perform the standby DCU processing as defined in 3.2.1:8 with the exception of functions (1)-(7) below:



3.2.1:9.3.1 Allowance for Power Interruption in the Cross-Channel (Continued)

- (1) Any tracking that requires use of the Inter-DCU Status Register.
- (2) CIE Inter-DCU Status Register Self-Test.
- (3) All OE self-tests.
- (4) Control Loop Tracking and update of any command ramps or timed command sequences.
- (5) Issuance of the Turn Off in-channel OE A/B Power Control Switch I/O instructions to turn off the 2 khz excitation, solenoid, servoswitch and igniter power supplies.
- (6) Processing of VEEI commands.
- (7) Any processing, other than scaling, that utilizes data coming from the cross-channel hardware components.

In addition, SEII monitoring will be suspended (3.2.3:6.1.3).

- (f) [IR316:1265;1] At each TRI, the time since item (a) shall be updated, and RCFI1, RCFI2, and ADPFI in the CIE shall be cleared, enabled, and their pending status and the PBD indication shall be examined:

- (1) [IR316:4468;1] If no RCFI1, RCFI2, or ADPFI pending indication or PBD is present, power has recovered in the other channel, then DCU A shall become the in-control DCU, and DCU B shall become the standby DCU.

If this is DCU B and Channel A power has returned, then DCU B will remain the standby DCU.

[IR317:4641;1] Else the in-channel is DCU A, and Channel B power has returned, then DCU A shall command all qualified OEs to the configuration of item (b).

3.2.1:9.3.1 Allowance for Power Interruption in the Cross-Channel (Continued)

[IR319] A Major Cycle Restart shall be executed per 3.2.1:2.3. [IR319:1394;1] Control loop computations shall be bypassed in the first major cycle. [IR319:3088;1] The power recovery of the cross-channel shall be reported with the associated response.

- (2) [IR320:3235;1] Else, if the time since item (a) is equal to or greater than 54 msec but less than or equal to 59 msec, the WDT closer to time-out shall be reset, and monitoring of ADPFI, PBD, RCFI1 and RCFI2 shall be performed until 59 msec from item (a). [IR321:1265;1] If RCFI1, RCFI2, ADPFI, and PBD indications are negated within this interval, power has recovered within limits, then the sequence of item (f) (1) shall be executed. [IR322] Otherwise, the sequence of item (f) (3) shall be executed.
- (3) [IR322:2270;1] When the duration of cross-channel power loss is greater than 59 msec, the OE On/Off Registers shall be immediately updated from the configuration set in item (b) to indicate cross-channel Power Off Time Exceeded. [IR324:3235;1] The OE Storage Registers Self-Test, 3.2.3:3.1.7, shall be suspended for this update. The cross-channel Power Off Time Exceeded indication will be set by loading the storage registers and transferring the contents. [IR324:5083;1] If RCFI1, RCFI2, ADPFI, and PBD are negated, the sequence of (f) (1) shall be executed. [IR324:5083;2] Else, if any are present, then the Engine/Controller On/Off Devices Self-Test, 3.2.3:3.2.3, shall be performed. This guarantees DCU self-disqualification if the OE cannot be updated to indicate cross-channel Power Off Time Exceeded. This check of the Power Off Time Exceeded status also serves as a support function of the PSE Logic/Redundancy Tests.

3.2.1:9.3.1 Allowance for Power Interruption in the Cross-Channel (Continued)

[IR325:1394;1] After a 0.5 msec wait to allow for any possible race, RCFI1, RCFI2, ADPFI, and PBD shall be rechecked. [IR326:1394;2] If all are negated, the sequence of item (f) (1) shall be executed.

[IR326:1386;1] Else, disqualification of the cross-channel DCU, and if applicable, the disqualification of the IE and OE, and DCU B Takeover, shall proceed, per 3.2.1:6.5.

[IR326:1208;2] Major Cycle Restart shall then be performed, per 3.2.1:2.3.

3.2.1:9.3.2 Power Loss After Cross-Channel DCU Disqualification

Power loss in a cross-channel after disqualification of its corresponding DCU is signaled by ADPFI or PBD, after the associated RCFI1 and RCFI2 have been disabled, i.e., after 3.2.1:9.

[IR331:1265;1] Once a cross-channel DCU has been disqualified for non-power reasons, the ADPFI will be cleared and enabled (see 3.2.1:2.3(h) (2)), and the PBD shall be polled each minor cycle.

[IR331:1265;2] If either the ADPFI pending indication, or PBD status indicates power loss, then the following shall be performed:

- (a) [IR332:1899;1] ADPFI shall be disabled and the polling of PBD each minor cycle shall be discontinued.
- (b) [IR332:4184;1] The failing IE and OE shall be disqualified per 3.2.1:6, unless previously disqualified.

### 3.2.2 Vehicle-Engine Interface

The Vehicle-Engine Electrical Interface (VEEI) functions of the Operational Program and/or PROM will provide for:

- (a) Receiving and executing commands for engine operation and checkout.
- (b) Reporting engine and controller status via a Vehicle Data Table (VDT).
- (c) Receiving and executing commands and data for loading data into memory.
- (d) Receiving readout commands and transmitting the requested data in lieu of the VDT.

A special firmware module, not directly included in the Operational Program, will provide some of the above functions. This module will be implemented in PROM and will be entered upon: receipt of a Reset Channel command, or power up when POI is set. The PROM software requirements are detailed in the PROM Spec.

- (e) When PROM has been entered, it will accept and process the following commands as described in the PROM spec.:
  - (1) Exit PROM
  - (2) FDR Cross-Channel Readout A
  - (3) FDR Cross-Channel Readout B
  - (4) FDR Enable A
  - (5) FDR Enable B
  - (6) Hello A
  - (7) Hello B
  - (8) IO Readout A
  - (9) IO Readout B
  - (10) Memory Load A
  - (11) Memory Load B
  - (12) Memory Load AB (PROM Rev 5 and subsequent versions)
  - (13) Memory Readout A
  - (14) Memory Readout B
  - (15) No Operation (PROM Rev 5 and subsequent versions)

3.2.2 Vehicle-Engine Interface (Continued)

- (16) PROM Sum Check A
- (17) PROM Sum Check B
  
- (18) RAM Sum Check A
- (19) RAM Sum Check B
  
- (20) RAM Write/Read Test A
- (21) RAM Write/Read Test B
  
- (22) Reset Channel A
- (23) Reset Channel B
  
- (24) Stop DCU A           (PROM Rev 5 and subsequent  
                                  versions)
- (25) Stop DCU B           (PROM Rev 5 and subsequent  
                                  versions)

Receipt of the Exit PROM command (after memory load if needed) will cause program execution to be transferred back to the Operational Program (in RAM). RAM execution is initiated at the address contained in the location specified in 3.3.4:2.

3.2.2:1 Vehicle Commands

Commands are received on the three Vehicle Command Channels (VCC) within the Vehicle Engine Electrical Interface (VEEI) and input by the DCU using the three VIE Command Register Channel A, B, and C I/O instructions. The contents of an individual input command register are changed by the corresponding vehicle command channel upon receipt of a new VCC transmission only. If the transmission satisfies the hardware checks, including correct BCH cyclic code, the new transmitted word is entered in the respective input command register. If the new transmission fails the checks, an all-zero word is entered in the respective input command register and remains unchanged until a transmission word has been received and validated by the hardware. In the absence of a new transmission or malfunction on an individual VCC, the corresponding input command register remains unchanged.

The Operational Program functions for vehicle command processing are command recognition and response, command voting, command acceptance, and execution of the commanded functions.

3.2.2:1.1 Command Recognition and Response

The Operational Program will periodically interrogate the input command registers to detect any change since their last interrogation. A change detected in the content of any input command register will initiate processing and response per the following:

- (a) [IR337] The Operational Program shall accommodate time skew of up to 1 msec in transmission between related updates of the three input command registers.
- (b) [IR337:1677;1] At the conclusion of the interval allowed for deskew, all three command registers shall be read and their contents will be voted on per paragraph 3.2.2:1.2 Command Voting.
- (c) [IR338] The Operational Program shall accommodate intervals between vehicle commands as short as 22 msec. Therefore, the interval between an interrogation of input command registers and the conclusion of deskew following the next interrogation must be less than 22 msec. [IR338:4785;1] Exceptions to this 22 msec requirement shall be allowed in response to memory readout, IO readout, when normal major cycle processing is suspended, and when the standby DCU performs IDSR/command confirmation. Suspension of major cycle processing occurs during a power transient, Controller Checkout, portions of Actuator Checkout, during Igniter Checkout, or during conditions that result in Major Cycle Restart. The commands that require the standby DCU to perform IDSR/command confirmation are: Enter Ground Checkout, Enter FRT-1, Enter FRT-2, Enter Flight, Purge Sequence 1, Purge Sequence 2, Purge Sequence 3, Purge Sequence 4, Start Enable, and Start.
- (d) [IR339] The response time from vehicle command receipt to start of the major cycle executing the command shall be no more than 25 msec. [IR340] The VDT report shall be initiated not more than 45 msec after vehicle command receipt and not more than 42 msec after command voting. [IR340:5469;1] Exceptions to these 25 and 42-45 msec requirements shall be allowed in response to a power transient on either channel, memory readout, IO readout, while in Controller Checkout, or to a Shutdown command in Start.

3.2.2:1.1 Command Recognition and Response (Continued)

- (e) [IR341:1699;1] Other than the exceptions (c) & (d), once a change has been detected in any VEEI command register and deskew provided for, processing of all channels per 3.2.2:1.2 and 3.2.2:1.3 shall be completed regardless of interruption to the normal program sequencing. This ensures that no vehicle command is lost.

When the PROM software is active it will periodically interrogate the input command registers to detect any change from their last interrogation. Examination for command voting and acceptability, execution of the command, and reporting of the outcome will be as defined in the PROM Spec.

3.2.2:1.2 Command Voting

Command voting will be performed following detection of a command receipt (by change in contents of any Vehicle Command Channel between two consecutive interrogations) and allowance for command skew. Following a Major Cycle Restart, command voting will be performed unconditionally (see 3.2.1:2.3(r)). Voting method and outcome will be as described below and in Table III.

- (a) [IR342:1826;2] A vote shall involve the comparison of the contents (word) of each of the Vehicle Command Channels with that of the other two channels. A majority command consists of either two non-zero Command Channel Words that agree and that word is not a Start command or Start Enable command, or three non-zero Command Channel Words that agree. See 3.2.1:8.1(f) (1) for the exception pertaining to the standby DCU.
- (b) [IR343:6153;1] Any one of the following conditions, checked in the listed priority, shall constitute a successful vote:
  - (1) The Single Command Channel Shutdown Enable timer has expired during Mainstage (which is Operational Data that is nominally equal to or greater than 512.86 seconds from Start) and no Shutdown Limit Control Inhibit has been in effect since the last Controller Reset command, and there is no new majority command and at least one Command Channel Word has changed since the last command vote and that word is either a Shutdown Enable or Shutdown command.
  - (2) Three Command Channel Words agree and are not zero.
  - (3) Two Command Channel Words agree and that word is not a Start command, Start Enable command, or zero. See 3.2.1:8.1(f) (1) for the exception pertaining to the standby DCU.

3.2.2:1.2 Command Voting (Continued)

- (c) When the vote is successful, per (b) above, the voted command is established based on the following criteria:
- (1) [IR343:6153;2] If the vote is successful, per (b) (2) or (b) (3) above, the agreed word shall become the voted command.
  - (2) [IR343:6153;3] If a Shutdown Enable command or a Shutdown command is the only Command Channel Word that was voted successfully per (b) (1) above, that word shall become the voted command.
  - (3) [IR343:6153;4] If both a Shutdown Enable command and a Shutdown command were voted successfully per (b) (1) above, the Shutdown shall become the voted command if a prior Shutdown Enable command is in effect on the same channel as the Shutdown command; otherwise, the Shutdown Enable shall become the voted command.
- (d) [IR343:4702;3] If the vote did not satisfy (b) above then that vote shall be declared a failed vote.
- (e) [IR343:6153;5] The outcome of the vote shall be reported per Table III.
- (f) [IR344:6153;1] Whenever a command voting failure occurs on any channel, the failure shall be reported; however, after Start in the Flight configuration, only one failure report per channel shall be reported until a Controller Reset command is executed.
- [IR344:6153;2] The command voting failures that shall be reported are as follows:
- (1) Any command channel that is zero
  - (2) All command channels if none agree
  - (3) The command channel that does not agree with the two command channels that do agree.
- [IR344:6153;3] No command voting failures shall be reported in the first major cycle following a Major Cycle Restart or anytime following a permanent channel power loss. This will prevent extraneous failure reports due to power interruption.
- (g) [IR345] No Vehicle Command Channel shall be permanently disqualified. If no new voted command can be obtained, engine operation will continue per the last implemented command.



3.2.2:1.2 Command Voting (Continued)

When the PROM software is active it will interrogate the Command Channels. If at least two Command Channel Words are the same and differ from the last previous voted command the vote is successful and the matched word will be used as the voted command.

3.2.2:1.3 Command Acceptance and Execution

[IR347:6153;1] The current voted command shall be checked for acceptance and placed in the VDT if any of the following conditions prevail:

- (a) A Shutdown Enable command or Shutdown command is the voted command per 3.2.2:1.2, (c) (2) or (c) (3)
- (b) A new majority command is the voted command;

otherwise no further processing of the current voted command shall be performed. The acceptance check will examine the voted command's command code, memory configuration, engine phase/mode and existing conditions.

[IR347:6153;2] If the voted command meets the acceptance criteria of Table V, then the command shall be accepted; otherwise the command will be rejected.

[IR347:6153;3] The necessary conditions for acceptance of a Shutdown command shall be as follows:

- (c) When the Shutdown command is a one out of three voted command, the previous voted command on the same channel must be a one out of three voted Shutdown Enable command with no intervening command channel changes, other than zero, between the two voted commands (see 3.2.2:1.2(b) (1)). When a Shutdown command from a Single Command Channel is accepted, a Single Channel Commanded Shutdown is reported for that channel.
- (d) When the Shutdown command is a majority command, the previous majority command must be a Shutdown Enable command (see 3.2.2:1.2(b) (2) and (3)).

[IR347:6153;4] If the voted command is a new majority command, including Shutdown Enable, all Single Command Channel Shutdown Enable commands that are in effect shall be negated. Single Command Channel Shutdown Enable commands may exist following a majority Shutdown Enable command.

[IR352:3300;1] The Command Status of the Engine Status Word (ESW) shall be updated according to whether the voted command is accepted or has been rejected.

3.2.2:1.3 Command Acceptance and Execution (Continued)

[IR354:5469;1] Functions to be executed in response to individual commands shall be as defined in Table V and the specific paragraphs referenced by the Table.

For the PROM, a successful voted command will be checked for acceptance and the status word updated per the PROM Spec.

3.2.2:1.4 Memory Loading Functions

Memory can only be loaded while in PROM. Operation of the PROM memory loader is described in the PROM Spec. The Operational Program does not have a load capability.

Subsequent to the completion of a memory load, a RAM Sumcheck or Exit PROM command will invoke the RAM Sumcheck function. Operation of this function is controlled by the Sum Check Address Table (SCAT), as described in 3.3.4:2.1.

3.2.2:2 Vehicle Recording Channel (VRC) Functions

The VRC Dual Port Memory Self-Test of 3.2.3:3.1.3 will be performed in conjunction with the update of the VRC DPMs.

3.2.2:2.1 Readout Capabilities

Memory Readout and IO Readout capability will be provided both in PROM and in RAM.

3.2.2:2.1.1 Readouts by the PROM Program

Main Memory, IE DPM, Input Words, and cross-channel FDR memory readout functions are provided in PROM. This provides the capability to dump the state of the Operational Program without executing in RAM. This capability is described in the PROM Spec.

3.2.2:2.1.2 Readouts by the Operational Program

[IR393:500206;1] The Operational Program shall provide the capability to read out IE DPM, Input Word Space, and Main Memory of either channel upon command while maintaining engine monitoring and control along with major cycle sequencing.

Caution must be exercised to avoid prefetching into data locations that are not decoded. If such a prefetch is made a Bus Error may occur.

3.2.2:2.1.2 Readouts by the Operational Program (Continued)

Command specific requirements are addressed in (a), (b), and (c); generic requirements are covered in (d).

(a) Readout of IE DPM

[IR395:500206;1] When an IO Readout Low IE DPM or IO Readout High IE DPM command is recognized as acceptable, the following shall occur:

- (1) [IR395:500206;2] The IE DPM being read out shall be from the channel requested by the command.
- (2) [IR395:500206;3] 128 contiguous IE DPM words shall be moved into the VRC DPM.  
[IR395:500206;4] For the IO Readout Low IE DPM command the starting address shall be \$820000.  
[IR395:500206;5] For the IO Readout High IE DPM command the starting address shall be \$820100.
- (3) [IR395:500206;6] Following the VDT which reports the IO Readout IE DPM command, a readout block shall replace the normal VDT contents for one VRC transmission.

(b) Readout of Input Words

[IR397:500206;1] When an IO Readout Input Space command is recognized as acceptable, the following shall occur:

- (1) [IR397:500206;2] The Input Words being read out shall be from the channel requested by the command.
- (2) [IR397:500206;3] Beginning with address \$820C00, 128 contiguous Input Space words shall be moved into the VRC DPM.
- (3) [IR397:500206;4] Following the VDT which reports the IO Readout Input Space command, a readout block shall replace the normal VDT contents for one VRC transmission.

(c) Readout of RAM

Readout of RAM is accomplished by transmitting two commands: a Memory Readout command followed by an encoded Starting Address command.

3.2.2:2.1.2 Readouts by the Operational Program (Continued)

The functional sequence is described in Table XLI. Requirements are as follows:

- (1) [IR399:500206;1] When a Memory Readout command is recognized by voting, both DCUs shall interpret the next voted command as the Starting Address command for the memory readout block. [IR399:500206;2] All subsequent vehicle commands shall be interpreted per the normal command code format regardless of whether the Memory Readout command was accepted.

[IR399:500206;3] A Starting Address command shall be accepted if all of the following conditions are met.

- (i) The Memory Readout command was accepted.
- (ii) The Starting Address command has a MSB of zero.

Codes for Starting Address commands were defined to minimize interpretation as vehicle commands if a Memory Readout command had not been detected.

- (iii) The Starting Address command is not between \$3FC0 and \$4000.

A 128 word read of RAM starting at a mapped address between \$00FF01 and \$00FFFF would violate prefetch restrictions.

- (2) [IR399:500206;4] The Starting Address command shall be reported in the VDT in a push-down stack per Table VI. It will appear in word 98 while the Memory Readout command will appear in word 99, if no subsequent command is accepted before VDT transmission. A rejected Starting Address command will not be used for readout, but will be reported in the VDT.

[IR399:500206;5] An accepted Starting Address command shall be mapped into the MC68000 address space by doubling the Starting Address command, sign extending it and redoubling it. The resulting mapped starting address will be the beginning location of the readout.

3.2.2:2.1.2 Readouts by the Operational Program (Continued)

- (3) [IR399:500206;6] If the Memory Readout and Starting Address commands are accepted, a readout block shall be formed and transmitted per the following:
  - (i) [IR399:500206;7] The memory being read out shall be from the DCU requested by the Memory Readout command.
  - (ii) [IR399:500206;8] Beginning at the starting address, 128 contiguous RAM words shall be moved into the VRC DPM.
  - (iii) [IR399:500206;9] Following the VDT which reports the Memory Readout and Starting Address commands, a readout block shall replace the normal VDT contents for one VRC transmission.

If the (vehicle) controlling system needs to ensure that the Starting Address command and its associated Memory Readout command appear in VDT Words 98 and 99 respectively, it must allow at least 44 msec between the Starting Address command and the next following command. This additional timing interlock, however, is not required by the Operational Program for proper memory readout.

(d) Generic requirements applicable to all readouts:

- (1) The following conditions will cause a rejection of a readout command:
  - (i) [IR401:500206;1] If any readout A command is received while a Switch VRC is in effect, the command shall be rejected.
  - (ii) [IR401:500206;2] If any readout A command is received while DCU A is disqualified, the command shall be rejected.

3.2.2:2.1.2 Readouts by the Operational Program (Continued)

- (iii) [IR401:500206;3] If any readout B command is received while DCU B is disqualified, the command shall be rejected.
- (2) [IR402:500206;1] If the memory being read out is that of the DCU which is the source of VRC data, the readout block contents shall replace the normal VDT contents for one VRC transmission. This applies to a readout A command if the Switch VRC is not in effect or a readout B command if the Switch VRC is in effect.
- (3) [IR405:5004;1] When a readout B command is received and DCU A is the source of VRC transmissions, DCU A will transmit a VDT and then shall switch control of the VRC over to DCU B. DCU B will initiate a single VRC transmission containing the requested memory readout data. The interval between any two VRC transmissions will be at least 38 msec, and the source of VRC data will not be changed during a VRC transmission.
- (4) [IR415:500206;1] The capability shall be provided to accommodate successive requests for readout blocks of either DCU in any combination. [IR416:500206;1] If the DCU to be read is the source of VRC data prior to the command, intervals as short as 88 msec between successive IO Readout or Starting Address commands shall be supported. [IR417:500206;1] If DCU A is in control and a readout B command is received while Switch VRC is not in effect, intervals as short as 166 msec between successive IO Readout or Starting Address commands shall be supported. In either case, intervals as short as 22 msec between any other two commands will be supported.
- (5) During memory readout operations, all functions of either DCU will continue uninterrupted except for the VDT transmission and interlocks specified above.

### 3.2.2:2.2 Vehicle Data Table Transmission

For the Operational Program, status data of the engine and controller as well as maintenance data will be regularly transmitted on the dual Vehicle Recorder Channels (VRCs). The data to be reported will be contained in the 128-word Vehicle Data Table (VDT). [IR423:2001;1] Data contents and requirements will be per the following subparagraphs, and shall pertain to the DCU that controls the VRC transmissions of the VDT data.

#### 3.2.2:2.2.1 VDT Contents

VDT data can be displayed in three formats. While in PROM a Dummy VDT format as described per the PROM Spec is utilized. While in the Operational Program either the standard VDT or the Actuator Checkout VDT form is used.

[IR424:6246;1] While in the Operational Program and Actuator Checkout mode is not active, data shall be reported as indicated in Table VI, Standard Vehicle Data Table. The first 32 entries are intended for use by the vehicle crew and for realtime telemetry. The rest of the table is primarily intended for later analysis. [IR424:4675;1] During the Actuator Checkout sequence of Table XXIV, data shall be reported as indicated in Table VII, Actuator Checkout Vehicle Data Table.

[IR424:3589;3] In the Operational Program VDTs all entries which can be expressed in engineering units shall be scaled, except for the data from sensors undergoing Sensor Checkout (reference Table XXVI, Part B, VDT word 95).

Entries requiring specific definitions are listed below; the others are self-explanatory.

- (a) [IR425:4588;1] The Engine Status Word (ESW), as defined by Table VIII, shall always reflect the state of the engine.
- (b) Time Reference is a count of major cycles reset (to zero) only when such response is explicitly called in this specification for individual commands or automatic events.

3.2.2:2.2.1 VDT Contents (Continued)

- (c) Failure Identification Word (Failure ID, Failure Delimiter) and Failure Parameter are as defined in 3.2.4 and Table I. The Failure Identification Words and Failure Parameters of the first three failures detected in a VDT period are reported in respective lists, as defined in 3.2.4.
- (d) [IR426] Vehicle Command: the two last successfully Voted Commands shall be entered in a push-down stack in VDT words 98 and 99.
- (e) When some parameters are dually-reported the first (lower Data Word Numbers) will be from the most recent major cycle, the second will be from the previous major cycle. This provides a 50 hz sampling rate for these parameters.
- (f) Selectable Entries are a special provision for additional data reporting during engine operation and testing. See 3.2.2:2.2.3 for specific requirements.
- (g) Checkout Test Step Number is the sequential number of the step being performed in a test sequence during a Component Checkout mode. When not in a Component Checkout mode, the content will be a selectable entry.

For the PROM, status data is transmitted on the dual recorder channels. The data to be reported is described in the PROM Spec.



3.2.2:2.2.2 VDT Processing

The VDT will always be transmitted simultaneously on both Vehicle Recorder Channels.

[IR432:1598;1] The VDT shall normally be transmitted in alternate major cycles. [IR432:1598;2] Specific timing within the major cycle shall ensure coherence of all data entries per 3.2.2:2.2.1 and maintenance of the transmission intervals at 40  $\pm$ 2 msec. (A 20 msec VDT capability will be provided for test purposes, 3.3.4:10).

Exceptions to the VDT interval requirements are allowed for cases involving interruption or suspension of major cycle sequencing, but should deviate as little as possible, within the specified constraints. The allowable cases include:

- (a) [IR433:4521;1] VDT interval limits shall be within 38 to 160 msec when any interruption in Major Cycle sequencing results in a Major Cycle Restart, or when the source of VRC data is switched from one DCU to the other.
- (b) [IR435:500206;1] Memory Readout and IO Readout: one VDT transmission shall be replaced by transmission of a single readout block.
- (c) [IR435:3974;1] During periods of Component Checkout where major cycles are suspended, timing between VDT transmissions shall be disrupted. These periods include Controller Checkout, Igniter Checkout, and during high sample rate monitoring of Actuator Checkout.

[IR438] Processing of VDT data by the in-control DCU shall ensure that no data in the VDT is altered while actual transmission is being executed by hardware. Where timing of data to be entered in the VDT cannot be predicted (e.g., Failure Identification and its associated data), appropriate buffering will be provided to satisfy this requirement.

### 3.2.2:2.2.2 VDT Processing (Continued)

[IR439] The current-value entries in the VDTs shall be the same as those current values used in the control and monitoring functions at the time of initiation of VDT transmission. Individual entries may be used in common between the VDT and other operational functions. When the VDT is from the standby DCU, some of the transmitted data may be more recent than that used in control and monitoring functions.

Processing requirements for other data parameters are limited to timely transfer to the VDT of the current parameter measurement inputs. [IR440:2168;1] The VDT data being reported shall be that which was input for use during the current major cycle. See 3.2.3:1.4.1 for definition of parameter measurement sampling.

VDT transmission requirements in PROM are described in the PROM Spec.

### 3.2.2:2.2.3 Selectable Entries of the VDT

The Vehicle Data Table (Table VI) defines a set of VDT data words as Selectable Entries. [IR441:1574;2] Data transmitted in these Selectable Entries shall be chosen via Operational Data (i.e., a pointer table). [IR442:6164;1] Prior to selection by Operational Data, the default Selectable Entries shall be as defined in Table VI.

### 3.2.2:2.2.4 Control of VDT VRC Transmissions

Nominally the in-control DCU is the source of VDT data transmitted to the vehicle. The Switch VRC and Restore VRC commands provide the vehicle the ability to select which DCU will be the source of VDT data. The following describes the response to these commands.

Requirements in this paragraph assume both DCUs are qualified and DCU A is the source of VRC transmissions initially. [IR444:1789;1] Subsequent to a Switch VRC vehicle command, DCU A shall output one more VRC transmission, switch control of VRC transmissions to DCU B, and then inform DCU B through the IDSR, per 3.2.3:3.1.2 that DCU B is now in control of VRC transmissions.

3.2.2:2.2.4 Control of VDT VRC Transmissions (Continued)

[IR444:2001;1] DCU B shall control the VDT transmissions upon confirmation that DCU A has relinquished control of VRC transmissions through the IDSR. [IR444:1789;2] Upon acceptance of a Restore VRC command, DCU B shall output one more VDT transmission. [IR444:4521;1] After DCU B has completed its final VRC transmission, but prior to DCU A VRC transmission, DCU A shall switch the source of VRC data to the DCU A VRC DPM. [IR444:1789;4] DCU A shall then inform DCU B of the switchover of the VRC source via the IDSR. [IR444:4521;2] DCU A shall not request a VRC transmission for at least 38 msec after DCU B has initiated its final VRC transmission.

Upon acceptance of a Controller Reset command, DCU A will take control of VRC transmissions, conforming to the timing constraints of 3.2.3:1.1.1, and then inform DCU B of the change of source of VRC data.

[IR448:1574;1] Upon disqualification of the cross-channel DCU, the in-channel DCU shall control VRC transmissions.

[IR448:1574;2] If DCU A is disqualified, then a Restore VRC command shall be unacceptable. [IR448:1574;3] If DCU B is disqualified, then a Switch VRC command shall be unacceptable.

[IR448:1574;4] If DCU B is the source of the VRC data, then a Switch VRC command shall be accepted, but no other action taken. [IR448:1574;5] If DCU A is the source of VRC data, then a Restore VRC command shall be accepted but no other action taken.

[IR448:1934;1] When a Switch VRC command is executed, an MCF shall be reported with the associated failure response (FID 20). The purpose of issuing an MCF is to emphasize that DCU B is now the source of VRC transmissions.

Significant differences in the VDT when it is being transmitted from the standby DCU include:

- (a) The Engine Status Word (ESW) may be generated by data available in DCU B and, as such, may differ from that generated by data available in DCU A. In particular the phase status, mode status and engine status bits may differ. Some examples of differences in the ESW are listed below:

3.2.2:2.2.4 Control of VDT VRC Transmissions (Continued)

- (1) The engine status bits may not reflect the true engine status because the standby DCU does not perform most engine monitoring.
  - (2) For commands which must be validated by phase/mode tracking before they are implemented in DCU B, the phase and mode status bits will not be updated until the validation is complete.
  - (3) Pneumatic or Hydraulic Shutdown initiated by DCU A (not initiated by a vehicle command) will not change the ESW in DCU B until the Shutdown has been validated by phase/mode tracking.
- (b) The data parameters resulting from IE DPM inputs, e.g., MCC Pc, reported in the DCU B VDT may be one major cycle older than the corresponding data being used by DCU A.
- (c) The confirmed failure information will reflect DCU B information. The standby DCU does not conduct many of the self-tests and engine monitor tests (reference 3.2.1:8).
- (d) The step value (VDT word 126) will not be updated during those checkout functions not performed by the standby DCU.

3.2.2:2.3 Failure Data Recorder (FDR) Readout

Readout of the cross-channel Failure Data Recorder (FDR) via the Vehicle Recorder Channel is provided by the PROM software. Requirements for the readout are described in the PROM Spec.

### 3.2.3 Engine Operations

The Operational Program is required to control the Space Shuttle Main Engine (SSME) during engine checkout operations and engine firing operations. During these operations the Operational Program will perform the applicable engine control and monitoring, self-tests, and failure responses.

The Operational Program can function in four different memory configurations. They are: Ground Checkout, FRT-1, FRT-2, and Flight. The Ground Checkout, FRT-1, and FRT-2 configurations perform engine checkout operations. The Flight configuration is used to control and sequence the engine during engine preparation and firing operations. Transitions between configurations are accomplished by appropriate Enter commands.

While the Operational Program can function in four different configurations, the engine operates in six engine phases. These phases are: Checkout, Start Preparation, Start, Mainstage, Shutdown, and Post Shutdown. The engine phases are in turn divided into modes. Table IX gives a synopsis of the functions of these modes. Table IV shows the possible engine phase/modes in each of the configurations.

There also is a PROM configuration with a PROM phase/Standby mode defined, but since it is not used by the Operational Program it will not be discussed in Table IX.

#### 3.2.3:1 Engine Control and Sequencing Operations

In order to control and sequence the engine during engine preparation and firing, the Operational Program must be in the Flight configuration. [IR449:3300;1] The Flight configuration shall provide all the capabilities specified under 3.2.1, 3.2.2, 3.2.3:1, 3.2.3:2.2, and 3.2.3:3 through 3.2.3:6, except as individually excluded in those paragraphs.

A typical engine phase sequence for the Flight configuration is shown in Figure 1.

Engine phases are entered upon acceptance of applicable commands of sequenced automatically per specified logic. Figures 2-6 illustrate sequencing between phase/modes.

### 3.2.3:1.1 Checkout Phase

The Checkout phase is the phase to which the Operational Program is initialized to begin active control, monitoring, or checkout of the SSME. This phase is entered upon acceptance of a Controller Reset or Checkout Standby command. Entry and sequencing through the Checkout phase are shown in Figure 2. The initial entry within this phase is into the Checkout Standby mode. The Checkout Standby mode is a waiting mode of engine operation during which active control sequence operations are not in progress.

#### 3.2.3:1.1.1 Controller Reset

[IR453:3550;1] The controller shall be reset to initial conditions as follows:

- (a) [IR453:3550;2] The phase/mode shall be set to Checkout Standby. [IR453:3300;1] The FRT mode shall be deactivated.
- (b) [IR463:2361;1] All failure indications, counts, status, and failure-related parameters shall be reset to indicate no failures; the failure lists (3.2.4:3) and CPU STOP Status buffer (3.2.1:6.1) shall be cleared; and the Self-Test Status field of the ESW shall be reset to Engine OK.
- (c) [IR465:3550;1] All components shall be assumed to be qualified until their possible disqualification during ensuing processing. [IR465:3550;2] However, the RCFIs and ADFFI shall remain in the enabled/disabled state that existed prior to the Controller Reset. This will be in effect until Major Cycle Initiation occurs.
- (d) All Inhibit (I) responses will be cleared.
- (e) [IR472:1789;1] A Switch VRC to DCU A I/O instruction (see Table XXXVIII) shall be issued at least 20 msec after acceptance of a Controller Reset command, but prior to a VRC transmission. [IR472:4521;1] DCU A shall not request a VRC transmission for at least 38 msec after DCU B has initiated its final VRC transmission.

3.2.3:1.1.1 Controller Reset (Continued)

- (f) A Controller Reset will not affect the state of any Operational or Adaptation data.
- (g) [IR475:1625;1] The default servoactuator (propellant valve) position and ramp rate to be used during the Engine Leak Detection Test Support (3.2.3:2.3.6) shall be set to 100% and 100%/sec, respectively. These values will be used unless overridden by the Set Propellant Valve Position or Set Propellant Valve Ramp Rate Command.
- (h) [IR475:1448;2] All fail-operational servoswitches shall be deenergized.
- (i) [IR475:2254;1] Major Cycle Initiation shall be entered per 3.2.1:2.2. A Major Cycle Restart will occur as a result of Major Cycle Initiation.
- (j) [IR475:3550;1] After completion of Major Cycle Restart, Checkout Standby mode functions shall be performed per 3.2.3:1.1.2.

3.2.3:1.1.2 Checkout Standby Mode

The Checkout Standby mode is a waiting mode of controller operation during which no active control sequence is in progress.

[IR476:1386;1] This mode shall be entered upon acceptance of a Checkout Standby command. It will also be entered upon acceptance of a Controller Reset command per 3.2.3:1.1.1 and will be the normal exit following the completion of tests performed in the Component Checkout modes as defined in the subparagraphs under 3.2.3:2.3.

[IR479:1448;1] The following shall be performed upon entry into Checkout Standby:

- (a) [IR479:3550;1] The phase/mode shall be Checkout Standby.
- (b) [IR479:3300;1] The FRT mode shall be deactivated.
- (c) [IR479:1395;4] The Shutdown Limit Control shall be enabled.

3.2.3:1.1.2 Checkout Standby Mode (Continued)

After the execution of items (a) thru (c) the appropriate bits of the Engine Status Word (ESW) and Identification Words of the VDT will be updated.

- (d) [IR479:1395;6] The running Time Reference of the VDT shall be reset to zero in the same VDT update as item (a) above.
- (e) [IR479:1395;7] All servoactuator (propellant valve) commands shall be set to the full closed position.
- (f) [IR479:1448;2] All solenoids, fail-safe servoswitches and igniters shall be deenergized.
- (g) [IR479:1448;3] The commanded power level shall be set to 100% RPL.
- (h) When entering from outside of Checkout Standby or by a Controller Reset command, SEII monitoring will be disabled for 9.50 +/- 0.04 sec (3.2.3:6.1.3).  
[IR479:5376;1] If the CCV SEII was disabled, the CCV SEII monitoring shall be resumed when the in-control servoactuator channel SEIIs are enabled.
- (i) [IR479:1448;5] Steps (a)-(h) above shall be performed in the same major cycle.

[IR479:2850;1] Following the delay of (h), the following shall be performed:

- (j) [IR479:2850;2] Servoactuator control shall be established as follows:
  - (1) [IR479:2850;3] If Checkout Standby was entered by means of a Controller Reset command, servoactuator Channel A shall be in control.
  - (2) [IR479:2850;4] Else, the in-control servoactuator channel shall remain in control.
- (k) SEII monitoring will return to the status defined in 3.2.3:6.1.3.

While in Checkout Standby, the memory configuration can be changed by an Enter command. [IR480:3300;1] When an Enter command is executed, the commanded memory configuration shall become the memory configuration of the Operational Program.



### 3.2.3:1.2 Start Preparation Phase

This phase is entered from the Checkout Standby or Post Shutdown Standby phase. The initial configuration of output devices at time of acceptance of command to enter the Start Preparation phase, is assumed to be the same as that defined in 3.2.3:1.1.2 for Checkout Standby mode. All solenoids, fail-safe servoswitches, and igniters will be deenergized. All servoactuator commands will be set to full closed position.

In this phase, system purges and propellant conditioning are performed in preparation for Engine Start, as shown in Figure 3. Four purge sequences are required to condition the engine.

The initiation and duration of each purge sequence is controlled by VEEI command. A specified set of operations will be performed upon the acceptance of each purge command on the VEEI. Subparagraphs 3.2.3:1.2.1 through 3.2.3:1.2.4 below define functions performed in response to each command in their nominal sequence. The sequence is also shown in Figure 3, with entry and exit conditions for each mode. The sequences described below assume that the purge sequence commands are received in their nominal order. [IR483] However, execution of any command accepted in any other allowable sequence shall result in the same output device configuration as that achieved with the nominal command sequence.

#### 3.2.3:1.2.1 Purge Sequence One Mode

[IR484] This mode shall be initiated upon acceptance of a Purge Sequence One command. [IR485:2964;1] Time Reference shall be reset to zero and the operations and functions of Table X, Part A performed.

#### 3.2.3:1.2.2 Purge Sequence Two Mode

[IR486] This mode shall be initiated upon acceptance of a Purge Sequence Two command. [IR487:2964;1] Operations and functions of this sequence shall be as described in Table X, Part B.

#### 3.2.3:1.2.3 Purge Sequence Three Mode

[IR488:1386;1] This mode shall be initiated upon acceptance of a Purge Sequence Three command or upon reversion from Purge Sequence Four or Engine Ready Mode. [IR489:3070;1] Operations and functions of this sequence shall be as described in Table X, Part C.

#### 3.2.3:1.2.4 Purge Sequence Four Mode

[IR490:2817;1] This mode shall be entered upon acceptance of a Purge Sequence Four command or upon reversion from Engine Ready mode. [IR491:3070;1] Upon acceptance of a Purge Sequence Four command, the operations and functions of Table X, Part D shall be performed. Upon reversion from Engine Ready mode, operations and functions of Table X, Part H (Purge Sequence Four Rollback) will be performed.

#### 3.2.3:1.2.5 Engine Ready Mode

[IR492] This mode shall be entered automatically upon satisfaction of both of the following conditions:

- (a) There is no I-response in effect, as described per 3.2.4:4 (i.e., all the I-responses are overridden by the appropriate number of Resume commands).
- (b) Conditions for Engine Ready are satisfied per 3.2.3:5.1.

Operations and functions while in this mode are described in Table X, Parts E, F & G.

[IR492:2817;1] If an I-response should occur during Engine Ready mode, reversion to Purge Sequence Four shall occur using the sequence of Table X Part H (Purge Sequence Four Rollback). An exception to this is reversion to Purge Sequence Three due to an RVDT miscompare.

[IR492:2817;2] Automatic reentry to Engine Ready from Purge Sequence Four shall occur upon satisfaction of both of the conditions (a) and (b). However, the out-of-limits Engine Ready sensor(s) which caused the reversion to Purge Sequence Four will not be monitored, 3.2.3:5.1.

#### 3.2.3:1.2.6 Start Enable

The Start Enable command is a precondition for acceptance of the Start command.

3.2.3:1.2.6 Start Enable (Continued)

- (a) A voted Start Enable command will be accepted provided:
  - (1) The CCV is at least 94% open,  
and either of the following is true:
    - (2) The current mode is Purge Sequence Four, no I-response is in effect, and all qualified Engine Ready sensors are currently within their respective Engine Ready limits (3.2.3:5.1),  
  
or
    - (3) The current mode is Engine Ready (3.2.3:1.2.5).
- (b) [IR495:1934;1] If the Start Enable command is rejected while the current mode is Purge Sequence Four with no I-response in effect, and at least one qualified Engine Ready sensor is out of limits, then the following shall occur:
  - (1) [IR495:1934;2] A failure response for each qualified sensor not currently within its respective Engine Ready limits shall occur.
  - (2) [IR495:1934;3] Each sensor reported under item (1) shall be removed from the list of sensors requiring Engine Ready monitoring.

When the command is accepted:

- (c) [IR496:1651;1] If not already in Engine Ready mode, Engine Ready mode shall be entered.
- (d) [IR497:986;1] The operations and functions of Table X, Part F shall be performed.
- (e) [IR503:2318;1] Start Enable shall be considered in effect until a new command has been voted, but not necessarily accepted, as defined in 3.2.2:1.2, or an I-response has occurred.
- (f) [IR504:1651;1] Upon acceptance of a command while in Start Enable, the following shall occur:
  - (1) [IR504:1651;2] If the accepted command is one which leads to another phase or mode, the command shall be implemented.

3.2.3:1.2.6 Start Enable (Continued)

- (2) [IR504:2817;1] If the accepted command does not lead to a new phase/mode, Start Enable shall be terminated and the operations and functions of Table X, Part G shall be performed.  
[IR504:2817;2] Upon acceptance of a subsequent Start Enable command, the 5 second suspension of Engine Ready monitoring and Purge and Ancillary monitoring, initiated in Table X, Part G, shall be terminated.
- (g) If an I-response occurs, the mode will revert to Purge Sequence Four via Table X, Part H (Purge Sequence Four Rollback). Reversion to Purge Sequence Three will occur if the I-response was due to an RVDT miscompare.

3.2.3:1.2.7 Termination of Purges by Command

Purge Sequence modes of Start Preparation can be terminated by other than the normal sequencing, through acceptance of specific commands. The phases/modes initiated by the respective commands are shown in Figure 3 and are as follows:

- (a) The Controller Reset command will initiate the Checkout Standby mode, per 3.2.3:1.1.1.
- (b) The Checkout Standby command will initiate the Checkout Standby mode, per 3.2.3:1.1.2.
- (c) Purge Sequence commands will initiate the applicable purge sequence mode, per 3.2.3:1.2.1 through 3.2.3:1.2.4.
- (d) The Terminate Sequence command will initiate the Terminate Sequence mode of Post Shutdown. Operations and functions of this mode are described in 3.2.3:1.6.1 and Table XV, Part A.
- (e) A Shutdown Enable command followed by a Shutdown command will initiate Pneumatic Shutdown per 3.2.3:1.5 and Table XIV.

3.2.3:1.3 Start Phase

Start phase comprises the operations that initiate engine firing. The phase begins with open-loop scheduling of propellant valves, then implements closed-loop control of MCC Pressure and Mixture Ratio for Mainstage operation.

### 3.2.3:1.3 Start Phase (Continued)

[IR512] Start phase shall be initiated upon acceptance of a Start command. [IR513:6038;1] Functions shall be executed according to the timed Start Sequence shown in Table XI. Initial conditions for this sequence are assumed to be those in effect at the end of Start Preparation phase.

[IR514:3074;1] Sequencing with other engine phases shall be as shown in Figure 4. Control loop functions are shown in Figures 8, 9, and 10.

### 3.2.3:1.4 Mainstage Phase

Mainstage phase comprises the operations to continue engine firing, including engine throttling in response to MCC Pressure Level commands. Closed-loop MCC Pressure and Mixture Ratio controls are maintained from Start phase.

[IR520:3074;1] Mainstage phase shall be automatically entered upon successful completion of Start phase and shall continue until initiation of Shutdown phase. [IR521] Phase entry and exit logic shall be as shown in Figure 4. [IR522:6038;1] Functions shall be executed according to the timed Mainstage sequence shown in Table XII. At the transition from Start to Mainstage, control loop integration and scheduled commands will be reinitialized to accommodate variable crossfeed gain, per Table XI Step 45, and 3.2.3:6.1.1. [IR522:4315;1] The OPOV and FPOV commands shall be reinitialized to the D/A output that is read via the IE.

[IR523:3074;1] The Operational Program shall be designed to provide the capability of maintaining Start/Mainstage phases for up to 2000 seconds.

#### 3.2.3:1.4.1 Control Loop Computations

Closed loop control is initiated in Start (Table XI). It is performed throughout Mainstage, and terminated in Shutdown (Table XIII and Table XIV). While the associated control loops are in effect, the propellant valves will be commanded to provide control of MCC Pc and propellant mixture ratio. [IR524:2266;1] The control functions shall be as described in Figures 8, 9, and 10, based on a major cycle of 20 msec, which results in an update rate of 50 hz. [IR525:1386;1] The computational lag shall be maintained within the limits indicated as follows, unless a Major Cycle Restart is required:

- (a) 15 msec for pressure parameters
- (b) 25 msec for temperature parameters

3.2.3:1.4.1 Control Loop Computations (Continued)

- (c) 35 msec for the propellant fuel flowrate parameter, above 50% RPL
- (d) 40 msec for the propellant fuel flowrate parameter, from 40% through 50% RPL

The computation lag is defined as the interval between sampling the applicable engine parameters and issuing the dependent control commands to the propellant valves. For pressure and temperature parameters, sampling is defined to occur upon completion of the Analog-to-Digital conversion of the sensor input signal. For flowrate parameters, sampling is defined as to occur upon completion of the actual measurement of the period of the sensor input wave.

[IR529:2049;1] Since the period of this wave is a function of flowrate, its computation lag requirement shall apply for 6.011 Mixture Ratio only and at MCC Pc levels where Mixture Ratio control is normally applicable.

[IR530] In performing the control function computations, the Tustin method shall be used to implement the transfer functions into sampled-data control equations, per 6.3.

3.2.3:1.4.2 MCC Pc Control

[IR531:1651;1] In response to acceptance of a Main Chamber Pressure Level command, the Pc control reference shall be updated under rate-limited control. [IR532:3074;1] The OPOV shall be commanded to drive measured engine MCC Pc to the commanded level under rate-limited conditions as shown in Figure 8. [IR533:2076;1] Cross-feed signals (as shown in Figure 8) shall also be provided to Mixture Ratio Control.

3.2.3:1.4.3 Mixture Ratio Control

[IR534:5950;1] Mixture ratio (6.011 nominal) shall be computed as the ratio of oxygen to hydrogen weight flowrates computed using the equations shown in Table XVI. [IR535:6038;1] The FPOV shall be controlled to achieve the desired mixture ratio, using the control laws shown in Figure 9.

3.2.3:1.4.4 Open Loop Control of CCV, MFV, and MOV

[IR536:2076;1] CCV, MOV, and MFV shall be controlled by the open loop laws shown in Figure 10. The scheduled commands used in controlling these propellant valves are specified in the Start Prep, Start, Mainstage, and Shutdown tables.

3.2.3:1.5 Shutdown Phase

Shutdown phase comprises the operations that reduce MCC Pressure and drive all valves closed to cease engine firing.

[IR538:4211;1] Upon acceptance of a Shutdown command while in the Start Preparation, Start, or Mainstage phase, the Shutdown phase shall be initiated. [IR538:5469;1] If the in-control DCU between Start + 0.80 sec and Start + 1.48 sec, and the standby DCU between Start + 0.76 sec and Start + 1.48 sec, accepts a Shutdown command, the Shutdown phase shall be delayed until Start + 1.50 sec. [IR538:3074;1] If a Shutdown command is accepted during Start Preparation phase, Hydraulic Lockup mode of Mainstage phase, or following an RVDT miscompare, then the Shutdown mode shall be Pneumatic; otherwise the Shutdown mode shall be Hydraulic.

[IR538:5456;1] Functions shall be executed according to the timed sequence shown in Table XIII for a Hydraulic Shutdown, or the sequence shown in Table XIV for a Pneumatic Shutdown. [IR539] Sequencing with other operating phases shall be as shown in Figure 5. [IR540:3074;1] No initial conditions are assumed; the design shall assure that proper Shutdown sequencing is achieved regardless of the prior phase and mode.

The Shutdown phase, either Hydraulic or Pneumatic, will also be initiated automatically per the following:

- (a) subsequent to a transition from PROM to RAM.
- (b) as a result of SSME or controller monitoring as described in 3.2.1:2, 3.2.3:5.2, 3.2.3:5.3, 3.2.3:6.1, and Table I.

See Servoactuator Error Indication Interrupt Monitoring (3.2.3:6.1.3) for monitoring and suspension of SEIIs during Pneumatic Shutdown.

3.2.3:1.5.1 Assured Pneumatic Shutdown

When a DCU is unable to initiate a normal Pneumatic Shutdown (see Table XIV), the Assured Pneumatic Shutdown must be invoked. To initiate an Assured Pneumatic Shutdown, both DCUs must be in the disqualified state in order to allow the power down matrix to initiate a Pneumatic Shutdown.

3.2.3:1.5.1 Assured Pneumatic Shutdown (Continued)

[IR542:5456;1] From the second major cycle through completion of the normal Pneumatic Shutdown sequence, if the in-channel OE has been disqualified or the cross-channel OE has been disqualified with the cross-channel Power Bus Down bit indicating power is present, the Emergency Shutdown solenoid and fail-safe servoswitches of the disqualified OE shall be monitored for failure to the ON state. [IR543:4934;1] If a failure to the ON state occurs, the DCU shall perform self-disqualification per 3.2.1:6.1.

3.2.3:1.6 Post Shutdown Phase

The Post Shutdown phase is entered automatically at completion of the Shutdown phase, after acceptance of a Terminate Sequence Command, or after a T-Response.

[IR549:2419;1] Sequencing with other operational phases shall be as shown in Figure 6. [IR550:1462;1] The Standby mode of this phase shall be entered automatically as shown in Figure 6.

[IR551:1843;1] While in Post Shutdown Standby, output devices shall be maintained as follows:

- (a) [IR551:1843;2] All solenoids, except for the Bleed Valve Solenoids, shall be deenergized.  
[IR551:1843;3] Fail-safe servoswitches and igniters shall also be deenergized.
- (b) [IR551:1843;4] If Post Shutdown Standby was entered via the Terminate Sequence command, the Bleed Valve Solenoids shall be deenergized. [IR551:1843;5] Else, if Post Shutdown Standby was entered from some other function (e.g., Hydraulic Shutdown, Pneumatic Shutdown, or PROM/RAM program memory), the Bleed Valve Solenoids shall be energized.
- (c) [IR551:1843;6] All servoactuator commands shall be set to full closed position.

The above output device configuration is the same as exists at normal completion of the mode leading to Standby.

If a Purge Sequence command is accepted while in this phase, the Start Preparation phase will be entered.



### 3.2.3:1.6.1 Terminate Sequence Mode

[IR554] Acceptance of a Terminate Sequence command shall initiate the Terminate Sequence mode of Post Shutdown phase. A Terminate Checkout Sequence Response (T-Response) will also initiate the Terminate Sequence mode. [IR555:4838;1] Applicable operations and functions shall be as described in Table XV, Part A. [IR556:4254;1] In addition, all indications to bypass Engine Ready monitoring for all parameters shall be reset.

### 3.2.3:1.6.2 Oxidizer Dump Mode

[IR557] Acceptance of a Oxidizer Dump command shall initiate this mode of the Post Shutdown phase. [IR559:3067;1] The sequence and timing for this mode shall be as defined in Table XV, Part B. Acceptance of a Terminate Sequence, Controller Reset, or Checkout Standby command will terminate this mode.

### 3.2.3:1.7 Engine On Failure Modes

Engine On Failure modes are the responses to detected failures during engine firing operations. Engine On Failure modes include Electrical Lockup, Hydraulic Lockup, Thrust Limiting and Fixed Density modes.

The Lockup modes are entered automatically in response to monitored failures of the SSME or controller. The conditions requiring such response are defined in 3.2.3:4.2, 3.2.3:6.1, and Table I.

There are two Lockup modes, Electrical Lockup and Hydraulic Lockup. [IR561:3070;1] Their sequencing with the other operating phases and modes shall be as shown in Figure 4.

Thrust Limiting mode will be initiated during Normal Control, or Fixed Density mode whenever the OPOV command exceeds its limit for the three consecutive major cycles. Engine control will change from Thrust Limiting mode back to Normal Control, or Fixed Density mode when the OPOV command has not exceeded its limit for three consecutive major cycles.

Fixed Density mode is entered during Start or Mainstage as a result of disqualification of both channels of LPFP Discharge Pressure or Temperature per 3.2.3:4.2.

### 3.2.3:1.7.1 Electrical Lockup

[IR564:1826;1] In this mode the servoactuator (propellant valve) commands shall be maintained at their last computed values prior to the initiation of Electrical Lockup. [IR565] All control loop computations shall be suspended.

[IR566:3070;1] The configuration of solenoids, servoswitches and igniters shall be commanded per the normal sequence for Mainstage.

[IR568] Exit from this mode, shall be to Hydraulic Lockup per 3.2.3:1.7.2 or to the Shutdown phase per 3.2.3:1.5, 3.2.3:5.3.1 and 3.2.3:5.4.1.

### 3.2.3:1.7.2 Hydraulic Lockup

[IR568:4473;1] If both servoactuator channels are not already disqualified, then both shall be considered to be disqualified upon entry into this mode. [IR569] In this mode all fail-safe servoswitches shall be deenergized immediately. [IR570] Execution of the OE commands shall satisfy the self-test requirements to verify correct loading of the OE Storage and OE On/Off registers. [IR572:4473;1] Solenoids and igniters shall be commanded as per the normal sequence for Mainstage. [IR573] All control loop computations shall be suspended. [IR574] The servoactuator (propellant valve) commands shall remain at the last values commanded prior to entering Hydraulic Lockup. SEII monitoring will be suspended (3.2.3:6.1.3).

The Hydraulic Lockup mode takes precedence over Electrical Lockup. [IR576] If a failure with Hydraulic Lockup response occurs during an Electrical Lockup mode, the Hydraulic Lockup mode shall be entered. [IR577:2049;1] If a failure with Electrical Lockup response occurs during an Hydraulic Lockup mode, the Electrical Lockup mode shall not be entered.

[IR578:2218;1] Exit from this mode shall always be to the fail-safe Pneumatic Shutdown mode; the Pneumatic Shutdown Sequence of Table XIV, shall then be executed.

[IR579:1642;1] Exit shall be in response to acceptance of a Shutdown command per 3.2.3:1.5, detection of a Shutdown Limit failure per 3.2.3:5.3.1 or detection of a FASCOS vibration failure per 3.2.3:5.4.1.

3.2.3:1.7.3 Thrust Limiting

OPOV and FPOV have command limits during Start, Mainstage and Shutdown.

- (a) When a computed OPOV or FPOV command exceeds its command limit, the command will be set to the specified command limit (See Table XI, Table XII, and Table XIII). During command limiting, Control Loop computations will continue.
- (b) [IR581:4399;1] Thrust Limiting mode shall be entered from Mainstage Normal Control or Fixed Density mode when the OPOV command is limited for 3 consecutive major cycles.
  - (1) [IR581:4399;2] Only the first occurrence of Thrust Limiting mode shall invoke the Thrust Limiting failure report indicated in Table I (FID 20).
  - (2) [IR581:5522;1] Pc Reference shall be used in place of MCC Pc in the Oxidizer Flowrate and Q Reference calculations while in Thrust Limiting mode. However calculation of the Oxidizer Flowrate coefficient  $C_2$  will use MCC Pc (Table XVI, Parts C and E).
  - (3) [IR581:4399;4] Recovery from Thrust Limiting mode back to Normal Control or Fixed Density mode shall occur when the OPOV command is not limited for 3 consecutive major cycles.
  - (4) [IR581:4399;5] Exit from the Thrust Limiting mode shall be to Electrical Lockup per 3.2.3:1.7.1, or to Hydraulic Lockup per 3.2.3:1.7.2, or to the Shutdown phase per 3.2.3:1.5, 3.2.3:5.3.1 and 3.2.3:5.4.1.
- (c) The OPOV Command Limit is computed as follows:
  - (1) [IR582:2270;2] From Start to Start + 3.58 sec, the OPOV Command Limit shall be 70%.

3.2.3:1.7.3 Thrust Limiting (Continued)

- (2) [IR582:2270;3] Beginning at Start + 3.6 sec, the OPOV Command Limit shall be computed as follows:

$$OCL = (A1 * EPL) + A0 + DCO$$

Where:

OCL is OPOV Command Limit in %.

A1 is a slope which is a function of EPL.  
EPL is Effective Power Level in % of Rated Power Level (RPL).

A0 is an offset which is a function of EPL.

DCO is Delta Command Offset in % and is nominally 0.0%.

- (i) [IR582:2982;5] A1 and A0 shall be functions of EPL as defined by:

	<u>EPL (% RPL)</u>	<u>A1</u>	<u>A0</u>
	0 ≤ EPL < 70	0.200	42.75
	70 ≤ EPL < 75	0.200	42.75
	75 ≤ EPL < 80	0.250	39.00
	80 ≤ EPL < 85	0.300	35.00
	85 ≤ EPL < 90	0.300	35.00
	90 ≤ EPL < 95	0.500	17.00
	95 ≤ EPL < 100	0.580	9.40
	100 ≤ EPL < 105	0.580	9.40
	105 ≤ EPL < 110	0.580	9.40
	110 ≤ EPL	0.960	-32.40

- (ii) [IR582:1651;6] EPL shall be computed as follows:

$$EPL = ((Pc \text{ Ref}) * 100.0/RPL) + ODPL$$

Where:

(Pc Ref) is MCC Pc Reference in psia.

RPL is Rated Power Level in psia.

ODPL is OPOV Delta Power Level in %.

3.2.3:1.7.3 Thrust Limiting (Continued)

- a. [IR582:2266;1] Prior to Start + 5.5 sec, ODPL shall be 9.65517%.
- b. [IR582:4550;1] At Start + 5.5 sec, ODPL shall be computed as follows:

$$\text{ODPL} = (\text{D1} * \text{M}) + \text{D0}$$

Where:

D1 is 1.5

D0 is -97.5

M is either the maximum OPOV position observed between Start + 5.02 and 5.5 sec, or 68%, whichever is greater.

A minimum value of 68% ensures that the minimum OPOV Command Limit at RPL shall be 70%.

- (3) [IR582:2982;6] If the OPOV Command Limit is computed to be greater than 100% by the above equation (i.e., (c) (2)) then the OPOV Command Limit shall be set to 100%.
- (4) [IR582:2270;4] The OPOV Command Limit shall be 100% in Shutdown. The OPOV Command Limit will be 100% in FRT-1 and FRT-2 in the Start and Mainstage phases.

3.2.3:1.7.4 Fixed Density

[IR583:5950;1] In the Fixed Density mode, a constant fuel density shall be used in all processing, as depicted in Table XVI, Part A(3).

### 3.2.3:2 Engine Checkout Operations

The engine checkout operations are performed to verify the operational status of engine components, and the overall flight readiness of the engine system. The Operational Program uses three memory configurations to perform these engine checkout operations. They are Ground Checkout, FRT-1, and FRT-2.

The Ground Checkout configuration is used to perform the engine component checkouts.

The FRT-1 and FRT-2 configurations verify the Operational Program is capable of firing the engine.

#### 3.2.3:2.1 Propellant Drop Monitoring

[IR593:1364;1] Monitoring for propellant drop (see 3.1.3:3.1.5) shall be performed by the in-control DCU to assure that no propellant is inadvertently present and that no dry gas spinning of flowmeters is occurring. [IR593:4785;1] Monitoring shall be performed except for the following conditions:

- (a) During Sensor Checkout mode.
- (b) During periods of Component Checkout where major cycles are suspended. These periods include Controller Checkout, Igniter Checkout, and during high sample rate monitoring of Actuator Checkout.
- (c) When the memory configuration is Flight.
- (d) During Terminate Sequence mode of Post Shutdown.
- (e) Upon acceptance of a command to either energize the Group 1 Sensor Checkout Switches or deenergize the Group 2 Propellant Drop Sensor Switches. Propellant Drop monitoring will be resumed per 3.2.3:2.3.6.

[IR593:3704;2] Disqualification of either OE shall not terminate propellant drop monitoring. When an OE is disqualified the Group 2 Propellant Drop Sensor Switch cannot be activated. Because the Propellant Drop monitoring is still active, the parameters will appear to violate Propellant Drop limits. This forces a Propellant Drop failure which in turn places the engine in a safe state.

3.2.3:2.1 Propellant Drop Monitoring (Continued)

[IR593:1364;3] While this monitoring is in effect, individual sensors of the following parameters shall be verified to be within the specified limits (f)-(h). Qualification of the respective sensors will be performed per 3.2.3:4.2.5.

- (f) [IR594:1364;1] LPFP Discharge Temperature shall be verified to be between \$BD48 (390R, Adaptation Range = +50R) and \$D238 (700R, Adaptation Range = +50R) (inclusive).
- (g) [IR595:1364;1] Preburner Pump Discharge Temperature shall be verified to be between \$DF08 (390R, Adaptation Range = +50R) and \$E4F8 (700R, Adaptation Range = +50R) (inclusive).
- (h) [IR596:1598;1] If a 16-bit Fuel Flowrate reading is not a saturation value (i.e., \$0000 or \$FFFF), the 15 LSBs of the Fuel Flowrate reading shall be verified to be greater than or equal to \$6C66. This will correspond to a Fuel Flowrate of 12 hz or less.

[IR596:1364;2] Monitoring of the LPFP Discharge Temperature and Preburner Pump Discharge Temperature shall be performed each major cycle. [IR596:1364;3] Monitoring of the Fuel Flowrate shall be performed within the major cycle in which an update is detected.

[IR597:2248;1] If any temperature sensor measurement is detected outside its specified limits for 3 consecutive major cycles, a Terminate Checkout Sequence failure response and report shall be executed as defined in 3.2.4:4. [IR597:1364;2] A single successful monitoring test of a temperature sensor prior to 3 consecutive strikes shall cancel all previous strikes.

[IR597:2248;2] If any Fuel Flowrate sensor measurement is detected outside its specified limits for 3 consecutive updates, a Terminate Checkout Sequence failure response and report shall be executed as defined in 3.2.4:4.

[IR597:1364;4] All strikes against a Fuel Flowrate sensor shall be cancelled if, prior to accumulating 3 consecutive strikes, either (i) or (j) is true.

3.2.3:2.1 Propellant Drop Monitoring (Continued)

- (i) A sensor measurement was within the limits specified in (h).
- (j) There had been at least 8 major cycles in which the sensor value had not been updated.

[IR600] The limits specified above shall be independent Adaptation Data constants alterable at time of loading only.

To perform the propellant drop monitoring as specified above, the measurement ranges of the LPFP and Preburner Pump Discharge Temperature sensors are expanded. This is accomplished by altering the circuit configuration of the temperature sensing channels. [IR601] Therefore, the Operational Program shall command the Group 2 (Propellant Drop Sensor) Switches on and the Group 1 (Sensor Checkout) Switches off throughout the engine control modes where this monitoring is to be performed. This monitoring is performed on the actual sensor values.

3.2.3:2.2 Checkout Standby Mode Tests

[IR603:591;1] The tests described in the following subordinate paragraphs are those that shall be performed in Checkout Standby. [IR603:591;2] These tests shall be performed each major cycle in addition to the tests described under Controller Continual Self-Tests.

3.2.3:2.2.1 DCU Exception Processing Test

The purpose of this test is to verify that specific exceptions can be generated and that the proper logic services those exceptions. Exceptions addressed by this test are those which may be generated under software control, and which are not tested elsewhere.

If necessary, performance of the test may be spread out among several major cycles with the test repeated in a cyclic fashion. [IR603:1386;3] This test shall be performed by both DCU A and DCU B.



3.2.3:2.2.1 DCU Exception Processing Test (Continued)

[IR603:591;7] The test shall invoke a targeted exception and verify the exception is serviced prior to the execution of the instruction after the instruction which generates the exception. [IR603:591;8] Failure of the exception to be serviced by the proper logic within this period shall constitute test failure. [IR603:591;9] If numerous conditions are listed that can invoke a given exception all conditions shall be tested. The exceptions to be tested and the exception generating conditions are as follows:

<u>Exception Vector Number</u>	<u>Assignment</u>	<u>Conditions</u>
3	Address Error	Reference to a word or long-word with an odd address
4	Illegal Instruction	Execution of ILLEGAL instruction (\$4AFC)
5	Zero Divide	Perform division by zero
6	CHK Instruction	Execution of CHK instruction such that the content of the subject register is less than zero or greater than content of location specified by effective address field
7	TRAPV Instruction	Execution of TRAPV instruction at a time when condition code indicates overflow

3.2.3:2.2.1 DCU Exception Processing Test (Continued)

8	Privilege Violation	Attempted execution of instructions ANDI to SR, EORI to SR, MOVE to SR, MOVE USP, ORI to SR, RESET, RTE, or STOP, while in the User State.
10	Illegal Vector	Execution of an instruction with \$A in bits 15 through 12
11	Illegal Vector	Execution of an instruction with \$F in bits 15 through 12
32-47 (inclusive)	Trap Instruction Vector	Execution of TRAP instruction with the corresponding exception vector encoded as 0 through 15 in bits 3 through 0

[IR603:591;10] During performance of this test, normal processing of these exceptions shall be suspended. [IR603:591;11] Processing of these exceptions during this test shall consist of merely indicating that the exception servicing logic was invoked.

[IR603:591;13] Failure of this test shall result in self-disqualification of the DCU/CIE.

3.2.3:2.2.2 PSE Output Voltages Maintenance Monitoring Test

The PSE Output Voltages Maintenance Monitoring Test verifies power supply output voltages that have not been checked elsewhere in the Operational Program. This test verifies that the voltages are within limits. [IR610:3;1] This verification shall be performed by both DCU A and DCU B.

3.2.3:2.2.2 PSE Output Voltages Maintenance Monitoring Test  
(Continued)

[IR610:4777;1] This test shall compare the input parameters in the IE DPM against the limits listed below:

<u>Parameter</u>	<u>Min Limit (Vdc)</u>	<u>Max Limit (Vdc)</u>
BATA1/BATB1	\$45D8 (2.7)	\$6878 (4.1)
CCPA/CCPB	\$A858 (-15.0)	\$D0D8 (-8.0)
AC+5MA/AC+5MB	\$6088 (5.2)	\$7698 (6.4)
C1P3/C2P3	\$5958 (4.6)	\$6708 (5.4)
C1M3/C2M3	\$3838 (4.4)	\$47D8 (5.6)
OE3A/OE3B	\$5378 (14.2)	\$5C68 (15.8)
DC+5MPA/DC+5MPB	\$5D38 (5.0)	\$7248 (6.2)
OE5A/OE5B	\$A398 (-15.8)	\$AC88 (-14.2)
CI1C/CI2C	\$5478 (4.4)	\$6BE8 (5.6)
LOG5A/LOG5B	\$5478 (4.4)	\$6BE8 (5.6)
CCPA-OE5A	\$03C0 (0.64)	N/A
CCPB-OE5B	\$03C0 (0.64)	N/A

Unscaled Cross-Channel Power Voltages, CCPA and CCPB, are verified to be greater than or equal to the unscaled OE5A and OE5B parameters, respectively, by a minimum of \$03C0 (0.64 Vdc).

3.2.3:2.2.2 PSE Output Voltages Maintenance Monitoring Test  
(Continued)

The monitoring of BATA1/BATB1 and CI1C/CI2C is a support function of the PSE Logic/Redundancy Tests.

A failure within this test occurs when a parameter is out of limits. [IR610:3;3] If two successive failures occur for the same parameter, the response shall be to report the parameter that failed. All failure reports are given in the PSE Logic/Redundancy Tests Support area of Table I.

3.2.3:2.3 Engine Component Checkout

[IR626] The in-control DCU shall satisfy the requirements stated herein. Standby DCU processing for engine component checkout is defined by 3.2.1:8.2.

Ground Checkout memory configuration is used to perform engine component checkout.

- (a) In the Ground Checkout memory configuration the following Component Checkout commands will be acceptable in Checkout Standby mode: Actuator Checkout, Controller Checkout, Engine Leak Detection, Igniter Checkout, Pneumatic Checkout, Sensor Checkout, and Hydraulic Conditioning.
- (b) [IR627:3300;1] When a Component Checkout command is executed, the associated Component Checkout mode shall be initiated. [IR627:4320;1] The Component Checkout modes shall be Actuator Checkout, Controller Checkout, Engine Leak Detection, Igniter Checkout, Pneumatic Checkout, Sensor Checkout, and Hydraulic Conditioning.
- (c) [IR628:3300;1] Upon entry to these modes, the ESW shall be updated accordingly, the Step Number (VDT word 126) initialized to 0, and the applicable functions/tests executed as defined in this section, 3.2.3:2.3. Setting the Step Number to 0 prevents misinterpretation with a previously executed checkout test.

3.2.3:2.3 Engine Component Checkout (Continued)

- (d) The functions of the Component Checkout commands are:
- (1) The Sensor Checkout command initiates checkout and calibration of the sensors and instrumentation system per 3.2.3:2.3.1.
  - (2) The Igniter Checkout command initiates checkout of the igniter system per 3.2.3:2.3.2.
  - (3) The Pneumatic Checkout commands initiate checkouts of the pneumatic system per 3.2.3:2.3.3.
  - (4) The Actuator Checkout commands initiate checkout of associated propellant valves and actuator systems per 3.2.3:2.3.4.
  - (5) The Controller Checkout command initiates checkout of the controller functions per 3.2.3:2.3.5.
  - (6) The Engine Leak Detection commands are used to support the engine leak checks per 3.2.3:2.3.6.
  - (7) The Hydraulic Conditioning command initiates an exercise of the hydraulic system and servoactuators per 3.2.3:2.3.9.
- (e) [IR630:2001;1] Upon completion of a test, a return to Checkout Standby mode shall occur.

[IR630:3300;1] When a verification test is specified, the indicated failure response shall be executed upon the first detection (strike) of the failure, unless specified otherwise.

There are two types of failures associated with the checkout tests: failures whose responses are specified in the checkout tests, and failures of higher order or unrelated controller components. [IR630:4526;1] During a Component Checkout mode, if an I-response occurs which is not a result of the checkout test, the checkout test shall be aborted and Checkout Standby shall be entered.

3.2.3:2.3 Engine Component Checkout (Continued)

[IR630:4699;1] Upon entry into a Component Checkout mode, any Failure Identification Word which is a result of the checkout test shall be reported only upon its first occurrence, and the associated monitoring shall be suspended. Thus, a duplicate Failure Identification Word can be reported if the checkout sequence is invoked again.

The Ground Checkout configuration will include the functions associated with the engine phase/modes specified in Table IV.

3.2.3:2.3.1 Sensor Checkout Test

[IR635:4844;1] This test shall be initiated upon acceptance of a Sensor Checkout And Calibration command, and the sequence of Table XXVI, Part A executed. This test will provide the outputs of all sensors to the VDT per format defined in Table XXVI, Part B.

The test verifies:

- (a) Sensor outputs for simulated operational conditions when Group 1A and 1B Sensor Checkout Switches are activated and Group 2A and 2B Propellant Drop Sensor Switches are deactivated.
- (b) Sensor outputs for ambient conditions when:
  - (1) Both Group 1A and 1B Sensor Checkout and Group 2A and 2B Propellant Drop Sensor Switches are deactivated.
  - (2) Group 1A Sensor Checkout and Group 2A Propellant Drop Sensor Switches are activated, and Group 1B Sensor Checkout and Group 2B Propellant Drop Sensor Switches are deactivated.
  - (3) Group 1A Sensor Checkout and Group 2A Propellant Drop Sensor Switches are deactivated, and Group 1B Sensor Checkout and Group 2B Propellant Drop Sensor Switches are activated.

3.2.3:2.3.1 Sensor Checkout Test (Continued)

The sequence allows for internal delays of the controller hardware. It also checks all sensor channel outputs to be within specified limits. [IR636:6164;1] Detected discrepancies shall be reported as defined in Table XXVI, Part C. [IR637:1608;1] During this sequence, sensor qualifying, and related failure responses, and control parameter computation per 3.2.3:4.2, 3.2.3:4.3 and 3.2.3:4.4, respectively, shall be suspended to avoid extraneous failure indications during switching between ambient and simulated conditions. [IR638] Sensor scaling shall be the only sensor processing performed. [IR639:6154;1] Following these checks, Preflight Calibration of all pressure sensors, except for Controller Internal Pressure and Hydraulic System Pressure Sensors, shall be performed.

[IR640] The Sensor Calibration function shall compute scale factor coefficients for the pressure sensors based on measurements in actual system operating conditions. [IR641] The calibration method and equations shall be as defined in Table XXVI, Parts A and D.

[IR642] The calibrated pressure sensor coefficients (obtained above) shall be stored. [IR643] The stored values shall be used by all configurations when sensor data scaling is performed.

[IR644] The locations containing these calibration coefficients shall be accessible as Adaptation Data constants.

[IR645] As the Sensor Checkout test is sequenced, the current step number as indicated in Table XXVI, Part A shall be entered in VDT Word 126. During this test all VDT entries which require sensor processing or computation other than sensor scaling will not be updated.

[IR645:2874;1] An I-response during Sensor Checkout which is a result of the test itself, shall not halt the checkout sequence. The checkout sequence will be allowed to continue to completion.

Upon completion of the checkout test sequence, the Operational Program will return automatically to the Checkout Standby mode.

3.2.3:2.3.2 Igniter Checkout Test

[IR647:3974;1] This test shall be initiated upon acceptance of a Spark Igniter Checkout command.

- (a) [IR647:3974;2] The Engine/Controller On/Off Devices Self-test of 3.2.3:3.2.3 shall be suspended until completion of the test.
- (b) The test is as follows:
  - (1) [IR647:3974;3] Subsequent to transmitting a VDT indicating Igniter Checkout has been entered, major cycle processing shall be suspended and both WDTs shall be maintained in the reset state until completion of the test.
  - (2) [IR647:4258;1] Both channels of all igniters shall be commanded On via the OE On/Off Registers as shown in Table XXXI.
  - (3) [IR647:3974;5] A delay of at least 40.0 msec shall be allowed for igniter monitor settling time.
  - (4) [IR647:4258;2] A series of six high speed monitoring periods, one for each channel of each igniter, shall be initiated.
    - (i) [IR647:4258;3] The duration of each monitoring period shall be 5 seconds.
    - (ii) [IR647:4258;4] Sampling shall be performed at least once every 70.0 usec. Input Words 15 and 16 provide igniter status data.
    - (iii) [IR647:4258;5] A failure shall be noted for each continual period of 30 +/-0 msec in which the igniter under test is indicated as being off.
  - (5) [IR647:4258;6] At the end of the last monitoring period, all igniters shall be commanded Off and major cycle processing resumed.

[IR647:3974;15] Failure indications of igniters shall be recorded but not reported during Igniter Checkout. [IR647:3974;16] Igniter failures detected during this test shall not halt the checkout sequence.



3.2.3:2.3.2 Igniter Checkout Test (Continued)

[IR647:4258;7] Failure reports and responses shall be made for all igniter failures recorded during the checkout in the first VDT transmission after resumption of major cycle processing. [IR647:4258;8] No more than one failure report shall be made for each channel of each igniter. [IR647:4258;9] The number of failures within the igniter monitoring period shall be reported in the Failure Parameter.

[IR647:3974;18] Upon completion of the test, the Engine/Controller On/Off Devices Self-test of 3.2.3:3.2.3 shall be restored after a minimum delay of 40.0 msec. The Operational Program will return to Checkout Standby.

3.2.3:2.3.3 Pneumatic Component Tests

Upon acceptance of one of the commands listed below, checkout tests on individual pneumatic components of the engine will be performed.

- . Checkout Fuel System Purge Control Valve
- . Checkout HPOP IMSL Purge Control Valve
- . Checkout Bleed Valve Control Valve
- . Checkout Emergency S/D Control Valve
- . Checkout Pogo Precharge Control Valve
- . Checkout Preburner S/D Purge Control Valve

[IR652:5768;1] When a Checkout Emergency Shutdown Control Valve command is accepted, an Actuator Pre-operational Conditioning Cycle per 3.2.3:2.3.8 shall be performed on all five actuators in parallel, followed by the Emergency Shutdown test sequence as defined in Table XXV. [IR652:4320;2] Upon acceptance of any other Pneumatic Checkout command, the applicable test sequence as defined in Table XXV shall be performed.

[IR653:3175;1] An I-response during Pneumatic Checkout, which is a result of the test itself, shall result in halting the checkout sequence at the step in which the failure was detected and de-energization of all pneumatic control valve solenoids.

3.2.3:2.3.3 Pneumatic Component Tests (Continued)

[IR653:4616;1] An appropriate Resume command shall restore the pneumatic control valve solenoids to the prefailure configuration. [IR653:4616;2] A delay as specified in Table XXV shall occur if re-energization of the pneumatic control valve solenoids is required. [IR653:4616;3] The Pneumatic Checkout sequence shall then resume at the step following the one in which the failure was detected.

[IR654] All position and pressure monitoring for the checkout sequences shall be performed on scaled values. [IR655:1503;1] Detected discrepancies relating to the specific checks performed by the commanded sequence shall be reported and responded to as defined in Table XXV. [IR656:2168;1] Failures detected by tests not specified by the Pneumatic Component Tests shall cause a response as normally applicable to such failures.

[IR658] As a test is sequenced the current step number, as indicated in Table XXV, shall be entered in VDT Word 126.

Upon completion of a test sequence, the Operational Program will return automatically to Checkout Standby.

3.2.3:2.3.4 Actuator Component Tests

Upon acceptance of one of the commands listed below, checkout tests on individual engine propellant valves will be performed.

- . Checkout MFV
- . Checkout MOV
- . Checkout CCV
- . Checkout FPOV
- . Checkout OPOV

When one of these commands is accepted:

- (a) [IR666:5386;1] The Emergency Shutdown solenoid and all fail-safe servoswitches shall be energized.

3.2.3:2.3.4 Actuator Component Tests (Continued)

- (b) [IR666:5386;2] After a delay of 2.0 seconds to vent pneumatic pressure, the fail-safe servoswitches shall be deenergized.
- (c) [IR666:4320;3] An Actuator Pre-operational Conditioning Cycle, per 3.2.3:2.3.8, shall be performed on all five actuators in parallel.
- (d) [IR666:5576;1] The applicable test sequence of Table XXIV shall be performed.

During Actuator Checkout the data reported in the VDT will be as indicated in Table VII.

During the checkout sequence, all fail-operational and fail-safe servoswitches will be commanded in accordance with Table XXIV. At the completion of the checkout sequence all fail-operational and fail-safe servoswitches will be deenergized.

[IR668:4139;1] Detected discrepancies relating to the specific checks performed by the commanded sequence shall be responded to and reported as defined in Table XXIV. [IR669] Other failures which may be detected while a test is being sequenced shall cause a response as normally applicable to such failures. This applies particularly to the Engine/Controller On/Off Devices Self-Test as defined under 3.2.3:3.2.3. SEII monitoring will be suspended while the test sequence is proceeding (3.2.3:6.1.3). In particular, individual servoactuator error indications will be disabled in the CIE except as specified in the sequence of Table XXIV.

[IR671:4699;1] While major cycle processing is in effect, the following shall be performed each major cycle during the Table XXIV sequence of Actuator Checkout:

- (e) [IR671:2262;2] The Hydraulic Pressure shall be monitored to be 2650 psia or greater. [IR671:4526;1] If IE B is temporarily or permanently disqualified, this test shall be bypassed. [IR671:4611;1] If the Hydraulic Pressure is out of limits for three consecutive major cycles, this shall constitute a failure.
- (f) [IR671:2262;3] The position of each actuator that is not under test shall be monitored to be less than or equal to 3% open. [IR671:4611;3] If this condition is not met, this shall constitute a failure.

3.2.3:2.3.4 Actuator Component Tests (Continued)

Failure Identification Words associated with the actuator component test are composed of 3 fields, the Failure ID, Valve ID, and Step Number. Valve IDs are shown below.

.	MFV	- ID	1
.	MOV	- ID	2
.	CCV	- ID	3
.	FPOV	- ID	4
.	OPOV	- ID	5

Step Numbers are defined in Table XXIV.

[IR671:4611;4] An I-response during Actuator Checkout, which is a result of the test itself or the Hydraulic Pressure Monitor, shall result in halting the checkout sequence at the end of the step in which the failure was detected unless otherwise stated within the test. [IR671:1422;2] An appropriate Resume command shall cause resumption of the Actuator Checkout sequence with the step following the one in which the failure was detected.

Upon completion of a test sequence, the Operational Program will return automatically to Checkout Standby.

3.2.3:2.3.5 Controller Checkout Tests

[IR675:1386;1] Upon acceptance of a Controller Checkout command each DCU shall suspend major cycle processing for execution of the Controller Checkout Tests as described in the following subordinate paragraphs. [IR675:591;2] This transition shall be coordinated such that no failures shall be induced by the transition process itself.

Characteristics of this environment include the following:

- (a) [IR675:591;3] Only processing described in this paragraph or as part of the subject Controller Checkout Tests shall be performed. As such, routine input of IE DPM data, monitoring and output of IDSR data as performed during major cycle operation, monitoring of VEEI command inputs, and output of VDTs from VRC DPM will not be performed.
- (b) Attempts to run Controller Checkout with only a single operational DCU will yield unpredictable results. The test sequence will abort. Similarly, all hardware components are assumed to be qualified.

3.2.3:2.3.5 Controller Checkout Tests (Continued)

(c) [IR675:1386;2] The following environment shall pertain prior to performance of each test:

- (1) [IR675:1386;3] Both DCUs shall perform the following in the given order (using I/O instructions per Table XXXVIII for i through v):
  - (i) Clear the SCP comparators.
  - (ii) Disable and clear all interrupts in the CIE.
  - (iii) Execute the Enable FDR Recording I/O instruction.
  - (iv) Force all WDTs to the timed-out state.
  - (v) Enable the SCPI.
  - (vi) Set the current interrupt level to zero.
- (2) Any interrupt processing environment differing from that stated above will be indicated in each test.
- (3) TRIs may be temporarily enabled and serviced for timing purposes as long as the occurrence of the interrupt and the logic that services it does not interfere with the environment of the test.
- (4) If a test refers to an interrupt indication, the interrupt indication may be considered for the purposes of Design, as either the actual occurrence of the interrupt or the corresponding pending bit.

(d) The protocols of paragraph 3.2.3:3.1.2 that describe the mechanics of IDSR data exchange may be suspended and replaced by protocols to be defined by Design. Provision will be made such that the in-channel DCU monitors the progress of the cross-channel DCU during the series of tests. Time-out values will be identified such that if the in-channel DCU does not progress within the test sequence as expected, the cross-channel DCU will detect this as a failure.

3.2.3:2.3.5 Controller Checkout Tests (Continued)

- (e) [IR675:2168;1] The subject tests shall be aborted and the failure shall be reported if either DCU detects any type of failure in the test being performed, including failure of Controller Continual Self-Tests (h-k). [IR675:591;14] Upon completion of all Controller Checkout tests or upon a failure detection, both DCUs shall perform Major Cycle Initiation, thereby reverting to Checkout Standby. [IR675:591;15] This transition shall be coordinated such that no failures shall be induced by the transition process itself. [IR675:5150;1] Prior to execution of Major Cycle Initiation, the following shall be performed:
- (1) Clear the SCP comparators.
  - (2) Issue a Reset +5V Under Voltage Test I/O instruction.
  - (3) Disable and clear all interrupts in the CIE.
  - (4) Execute the Enable FDR Recording I/O instruction.
  - (5) Force all WDTs to the timed-out state.
  - (6) Set the current interrupt level to four.
  - (7) Reinstate the interrupt enable/disable configuration in the CIE to the condition that prevailed prior to entry into Controller Checkout.
  - (8) Restore control of the VRC to the DCU that had control of it prior to the entry into Controller Checkout.
- (f) [IR675:4697;1] In the event of an unexpected exception vector, the normal processing shall be conducted with the resultant DCU disqualification. [IR675:4697;2] If an unexpected interrupt appears as either non-pending or not enabled, the normal processing shall consist of performing the Interrupt Decoder Self-Test of 3.2.3:3.1.5 which results in the disqualification of the DCU. [IR675:6245;1] If an unexpected interrupt is an enabled SCPI and is not a transient interrupt per 3.2.1:4(c), or is a PFI or PRI, the normal processing shall be conducted with the resultant DCU disqualification.
- (g) [IR675:591;22] Unlike other Component Checkout tests, the effect of a Resume command subsequent to a failure in Controller Checkout shall not cause a resumption of these tests when the I-response count has reached zero, rather the program shall remain in Checkout Standby.

3.2.3:2.3.5 Controller Checkout Tests (Continued)

During execution of the tests described in the following subordinate paragraphs, elements of certain continual self-tests will be performed. These elements are either specified as explicit test steps within the description of the given test, or are implicit in the performance of certain test steps. These implicit elements are limited to and specified as follows:

- (h) [IR675:591;24] During the process of IDSR data exchange while performing Controller Checkout, the transmitting DCU shall load its IDSR, then read its IDSR contents. [IR675:591;25] If the loaded and read values do not match, this shall constitute test failure.
- (i) [IR675:591;26] For each occurrence of the OE Storage Register, the program shall load the register, then read its contents (see Table XXXVII). [IR675:591;27] If the loaded and read values do not match this shall constitute test failure.
- (j) [IR675:591;28] For each occurrence of transferring the content of an OE Storage Register for which the state of an on/off device(s) is being changed, the program shall delay an amount of time required such that the switched device or devices can be monitored. The program will then verify all on/off devices to be that which is expected. [IR675:591;29] Failure to verify the expected states shall constitute a test failure. On/off devices and delay times to be used in this test are as specified in 3.2.3:3.2.3, Engine/Controller On/Off Devices Self-Test.
- (k) [IR675:591;30] For each occurrence of an IE input sequence the program, after loading the IE Address and Range Counters and prior to initiating the request, shall read the contents of these counters (see Table XXXVII). [IR675:591;31] Failure of the loaded and read values to be equal or failure of the channel indicator to be zero shall constitute test failure.

Upon completion of the IE input sequence, the IE Address and Range Counters will again be read via input words. [IR675:591;32] If the value in the IE Range Counter is non-zero, or the value in the IE Address Counter is not

3.2.3:2.3.5 Controller Checkout Tests (Continued)

equal to the sum of the initial IE Address Counter plus the initial IE Range Counter contents, or if the conversion complete indication does not exist, or if the channel indicator indicates Channel A then the test shall be declared a failure.

The input of each parameter pair takes 50 usec with at least an additional 50 usec for termination conditions.

Whenever a test or verification is required to be made at a point expressed as X +/- Y time units, it is required that the software make its test/verification only at any one point in time within this range. [IR675:591;35] Based on that single sample, the step shall pass or fail.

The following subordinate paragraphs detail the Controller Checkout tests. [IR675:4597;1] Each receipt of the Controller Checkout command shall start the test sequence with the first test. [IR675:591;36] The Operational Program shall execute these tests in the order that they are specified. This provides a degree of fault isolation.

3.2.3:2.3.5:1 SCP Comparator Test

The purpose of the SCP Comparator Test is to verify that both data bus and address bus comparators will detect mismatches on each bit of their respective buses. The test is accomplished by using the SCP mismatch test word in PROM and the data of the following two tables to generate unique mismatches of each bit on the DCU address and data bus (excluding address bus bits which would cause a bus error exception). The PROM mismatch word contains \$0000 for MPU1 and \$0001 for MPU2. [IR675:1386;8] This test shall be performed by both DCU A and DCU B.

(a) The data bus comparator test sequence is as follows:

- (1) [IR675:1386;9] The SCPI shall be disabled.
- (2) [IR675:591;38] The PROM mismatch word shall be fetched from address \$800FFE and retained in a register for later use. This will cause a mismatch corresponding to case number 1 of the first ensuing table which contains data mismatch patterns.



3.2.3:2.3.5:1 SCP Comparator Test (Continued)

- (3) SCP MPU One and Two Data and Address Error status will be verified (see Table XXXVII) to indicate data errors for both MPUs and not indicate an address error for either MPU. [IR675:591;39] Absence of either data error indication or the presence of an address error indication shall constitute failure of this test.
- (4) [IR675:591;40] The SCP comparators and SCPI shall be cleared.
- (5) [IR675:1386;10] The miscompare data fetched in step (2) shall be used to generate a miscompare pattern that corresponds to the next case of the first ensuing table; this pattern shall be written to a memory location to cause a miscompare.
- (6) SCP MPU One and Two Data and Address Error status will be verified to indicate data errors for both MPUs and not indicate an address error for either MPU. [IR675:591;42] Absence of either data error indication or the presence of an address error indication shall constitute failure of this test.
- (7) [IR675:591;43] The memory location into which the pattern was written shall be cleared of miscompare data.
- (8) [IR675:591;44] The SCP comparators and SCPI shall be cleared.
- (9) [IR675:1386;11] Steps (5) thru (8) above shall be executed for each of the data miscompare patterns of the first ensuing table.
- (10) [IR675:4597;2] The first or next address miscompare pattern of the second ensuing table shall be generated from the PROM miscompare word fetched in step (2) and shall be used as an operand address. [IR675:4597;3] The byte at the operand address shall be read and retained. [IR675:4597;4] Because an address miscompare and possibly a data miscompare will occur, the SCP comparators and SCPI shall be cleared.

3.2.3:2.3.5:1 SCP Comparator Test (Continued)

- (11) [IR675:4597;5] Any bit pattern shall be written to the byte location of the operand address. This ensures that identical data written to the miscompare addresses will cause only address miscompares.
- (12) [IR675:591;48] SCP MPU One and Two Data and Address Error status shall be verified to indicate address errors for both MPUs and not indicate a data error for either MPU. [IR675:591;49] Absence of either address error indication or the presence of a data error indication shall constitute failure of this test.
- (13) [IR675:4597;6] The retained data byte shall be restored to the operand address. An address miscompare and possibly a data miscompare will occur.
- (14) [IR675:1386;13] Steps (10) through (13) above shall be executed for each of the address miscompare patterns defined in the second ensuing table.

[IR675:591;52] After completion of this test, the DCU MPUs shall be cleared of any miscompare data. The initialization by 3.2.3:2.3.5(c) will clear the SCP comparators and the SCPI before execution of the next test.

3.2.3:2.3.5:1 SCP Comparator Test (Continued)

## DATA MISCOMPARE PATTERNS

<u>NUMBER</u>	<u>MPU1</u>	<u>MPU2</u>
1	\$0000	\$0001
2	\$FFFF	\$FFFE
3	\$0000	\$0002
4	\$FFFF	\$FFFD
5	\$0000	\$0004
6	\$FFFF	\$FFFB
7	\$0000	\$0008
8	\$FFFF	\$FFF7
9	\$0000	\$0010
10	\$FFFF	\$FFEF
11	\$0000	\$0020
12	\$FFFF	\$FFDF
13	\$0000	\$0040
14	\$FFFF	\$FFBF
15	\$0000	\$0080
16	\$FFFF	\$FF7F
17	\$0000	\$0100
18	\$FFFF	\$FEFF
19	\$0000	\$0200
20	\$FFFF	\$FDFE
21	\$0000	\$0400
22	\$FFFF	\$FBFE
23	\$0000	\$0800
24	\$FFFF	\$F7FE
25	\$0000	\$1000
26	\$FFFF	\$EFFF
27	\$0000	\$2000
28	\$FFFF	\$DFFF
29	\$0000	\$4000
30	\$FFFF	\$BFFF
31	\$0000	\$8000
32	\$FFFF	\$7FFF

3.2.3:2.3.5:1 SCP Comparator Test (Continued)

## ADDRESS MISCOMPARE PATTERNS

<u>NUMBER</u>	<u>MPU1</u>	<u>MPU2</u>
1	\$000000	\$008000
2	\$FFFFFF	\$FF7FFF
3	\$000000	\$004000
4	\$FFFFFF	\$FFBFFF
5	\$000000	\$002000
6	\$FFFFFF	\$FFDFFF
7	\$000000	\$001000
8	\$FFFFFF	\$FFEFFF
9	\$000000	\$000800
10	\$FFFFFF	\$FFF7FF
11	\$000000	\$000400
12	\$FFFFFF	\$FFFBFF
13	\$000000	\$000200
14	\$FFFFFF	\$FFFDFF
15	\$000000	\$000100
16	\$FFFFFF	\$FFFEFF
17	\$000000	\$000080
18	\$FFFFFF	\$FFFF7F
19	\$000000	\$000040
20	\$FFFFFF	\$FFFFBF
21	\$000000	\$000020
22	\$FFFFFF	\$FFFFDF
23	\$000000	\$000010
24	\$FFFFFF	\$FFFFEF
25	\$000000	\$000008
26	\$FFFFFF	\$FFFFF7
27	\$000000	\$000004
28	\$FFFFFF	\$FFFFFB
29	\$000000	\$000002
30	\$FFFFFF	\$FFFFFD

3.2.3:2.3.5:2 SCP Interrupt Test

The purpose of the SCP Interrupt Test is to verify, when a DCU bus miscompare is detected, that the SCP comparators will generate an SCP interrupt, force immediate time-out of the WDTs and inhibit update of the Failure Data Recorder. This test also verifies the operation of the SCPI CIE interrupt mask register bit and the SCPI pending status bit. The test is accomplished by forcing a DCU data bus miscompare by reading the SCP miscompare test address in PROM and then verifying proper behavior of the SCPI, WDT time-out, FDR, and SCPI enabling/disabling.

[IR675:591;54] During the performance of this test, the logic that normally services an SCPI for a non-test failure shall be inhibited. [IR675:1386;14] This test shall be performed by both DCU A and DCU B.

(a) The test sequence is as follows:

- (1) [IR675:1386;15] Both watchdog timers shall be reset. [IR675:591;58] This shall be a one-time event.
- (2) [IR675:1386;16] The PROM miscompare word shall be fetched from address \$800FFE.
- (3) [IR675:1386;17] Failure of the SCPI to have occurred before the third instruction after execution of the instruction triggering the SCP miscompare shall constitute failure of this test.
- (4) [IR675:591;60] The WDT1/WDT2 Timed-Out and FDR Recording status shall be read (see Table XXXVII). [IR675:4381;1] Failure of either WDT status to indicate timed-out or failure of the FDR Recording to be inhibited shall be treated as failure of this test.
- (5) [IR675:591;62] Verify that the SCPI pending status indicates interrupt pending (see Table XXXVII). [IR675:591;63] Test failure shall occur if not pending.

3.2.3:2.3.5:2 SCP Interrupt Test (Continued)

- (6) [IR675:591;64] The SCP comparators and SCPI shall be cleared which sets the SCPI pending status to non-pending.
- (7) [IR675:591;66] Both WDTs shall be reset and the FDR Recording shall be enabled as another one-time event.
- (8) [IR675:6261;1] The contents of the PROM miscompare word shall be used as an index or displacement to create an address error.
- (9) [IR675:1386;19] Failure of the SCPI to have occurred before the third instruction after the execution of the instruction triggering the SCP miscompare shall constitute failure of this test.
- (10) [IR675:591;68] The WDT1/WDT2 Timed-Out and FDR Recording status shall be read. [IR675:4381;2] Failure of either WDT status to indicate timed-out or failure of the FDR Recording to be inhibited shall be treated as failure of this test.
- (11) Verify that the SCPI pending status indicates interrupt pending. [IR675:591;70] Test failure shall occur if not pending.
- (12) [IR675:591;71] The SCPI shall be disabled in the CIE.
- (13) Test that the SCPI pending status indicates interrupt not pending. [IR675:591;72] Test failure shall be reported if pending is indicated.
- (14) [IR675:591;73] The SCP comparators and SCPI shall be cleared.
- (15) [IR675:591;74] The SCPI shall be enabled in the CIE.
- (16) Test that the SCPI pending status is still indicating interrupt not pending. [IR675:591;75] If pending, the test shall be declared failed.

[IR675:591;77] After completion of this test all miscompare data shall be eliminated from the MPUs and main memory.

3.2.3:2.3.5:3 DTACK Monitor/Bus Error Generator Test

The purpose of the DTACK Monitor/Bus Error Generator test is to verify that the DTACK monitor/bus error generator will force the SCP microprocessors into bus error exception processing whenever an undefined address is accessed. The test is to be accomplished by exercising all of the unused address bits and verifying occurrence of the Bus Error exception.

[IR675:1386;20] This test shall be performed by both DCU A and DCU B.

[IR675:591;79] During the performance of this test, the logic that normally services the error exception for a non-test failure shall be inhibited. Processing of the exception will consist primarily of verifying that the exception processing was invoked.

(a) The test sequence is as follows:

- (1) [IR675:1386;21] The SCPI shall be disabled in the CIE.
- (2) [IR675:4102;1] A long-word read or write access shall be performed for the following illegal address:

\$010000	Read
\$FEFFFE	Write

- (3) Failure of a bus error exception to occur will suspend the in-channel DCU which results in no error indication being reported by the DCU that failed. However, the cross-channel DCU will issue a Controller Checkout Protocol Procedure failure report designating that the in-channel DCU has timed-out during the test (see Table II).

3.2.3:2.3.5:4 VRC DPM Write/Read Test

The purpose of the VRC DPM Write/Read Test is to verify that bit patterns of both polarities can be written into and read from each of the VRC DPM addresses (word addresses \$820600 through \$8206FE) and to verify that each VRC DPM address can be uniquely addressed.

[IR675:1386;24] This test shall be performed by both DCU A and DCU B.

[IR675:1386;25] All VRC DPM words shall be set to a predetermined pattern other than \$5555 and \$AAAA prior to initiation of the test sequence.

3.2.3:2.3.5:4 VRC DPM Write/Read Test (Continued)

[IR675:591;86] The test shall be accomplished by writing, then reading both \$5555 and \$AAAA test bit patterns into a VRC DPM address. [IR675:4597;7] After each test bit pattern is written into a VRC DPM address, the test routine shall also verify that the predetermined pattern has not been altered in any other VRC DPM address. [IR675:1386;26] When a VRC DPM address has been tested successfully, it shall be rewritten with the predetermined pattern before the next VRC DPM address is tested.

[IR675:4597;8] If the proper bit pattern is not successfully read back or if the predetermined bit pattern has been altered in a non-subject VRC DPM location, the test shall be considered failed.

3.2.3:2.3.5:5 VRC Output Test

The purpose of this test is to verify that each VRC can output 128 words of data to the vehicle within the proper time allowances. It also verifies proper operation of VRC address registers and output complete indicators.

[IR675:1430;1] This test shall be performed by both DCU A and DCU B each while operating as the in-control DCU. For the in-control DCU, WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running.

(a) The test is conducted per the following steps.

- (1) [IR675:4777;1] The Phase and Mode fields of the ESW shall be set to Checkout and Controller Checkout respectively. [IR675:591;90] The Initiate VRC Data Transmission I/O instruction shall be executed (see Table XXXVIII).
- (2) [IR675:591;91] The in-control DCU shall continually monitor the VRC address registers corresponding to the in-control DCU's VRC DPMs and the corresponding complete indicators (see Table XXXVII).  
[IR675:4381;3] It shall verify that the address registers are zero and that the complete indicators indicate the not complete state within 2 +3/-0 usec from the output initiation of step 1.  
[IR675:591;93] Failure to verify these items shall constitute test failure.



3.2.3:2.3.5:5 VRC Output Test (Continued)

- (3) [IR675:1386;28] The in-control DCU shall continue to monitor the corresponding address registers and shall verify that they achieve the value of one, within  $19 +21/-2$  usec from the output initiation of step 1. [IR675:591;95] Failure to verify this shall constitute test failure.
- (4) [IR675:591;96] The in-control DCU shall continue to monitor the corresponding address registers and shall verify that they achieve each intermediate value (in increments of 1) from 0 through \$7F, within  $2.432 +0.050/-0.030$  msec of the output initiation in step 1. [IR675:591;97] Failure to achieve all intermediate values or \$7F within the specified time shall result in test failure.
- (5) [IR675:591;98] The in-control DCU shall continue to monitor the corresponding address registers and shall verify that they achieve a value of zero and that the corresponding complete indicators indicate the complete state within  $19 +6/-6$  usec of the time that the corresponding address register achieves a value of \$7F in step 4.

3.2.3:2.3.5:6 IE DPM Write/Read Test

The purpose of the IE DPM write/read test is to verify that bit patterns of both polarities can be written into and read from each of the IE DPM addresses (word addresses \$820000 through \$8201FE).

[IR675:1386;29] This test shall be performed by both DCU A and DCU B.

[IR675:1386;30] All IE DPM words shall be set to a predetermined pattern other than \$5555 and \$AAAA prior to performance of this test.

[IR675:591;101] The test shall be accomplished by writing, then reading both \$5555 and \$AAAA test bit patterns into an IE DPM address. [IR675:4597;9] After each test bit pattern is written into an IE DPM address, the test routine shall also verify that

3.2.3:2.3.5:6 IE DPM Write/Read Test (Continued)

the predetermined pattern has not been altered in any other IE DPM address. [IR675:1386;31] When an IE DPM address has been tested successfully, it shall be rewritten with the predetermined pattern before the next IE DPM address is tested.

[IR675:4597;10] If the proper bit pattern is not successfully read back or if the predetermined bit pattern has been altered in a non-subject IE DPM location, the test shall be considered failed.

3.2.3:2.3.5:7 IE Address Counter Test

The purpose of this test is to verify that each bit of both IE Address Counters can be toggled.

[IR675:1386;32] This test shall be performed by both DCU A and DCU B.

[IR675:591;105] The requirement of 3.2.3:2.3.5 (k) to verify the loaded content of the IE Address Counter shall be superseded by the steps of this test.

[IR675:1386;33] The IE Address Counter test shall be accomplished by writing then reading a rotating bit pattern, as shown in the following table through the in-channel IE Address Counter (see Table XXXVII). [IR675:591;107] Failure to read the expected input pattern shall constitute failure of this test.

<u>PATTERN</u>	<u>OUTPUT TO IE ADDRESS COUNTER (BITS 7-1)</u>	<u>EXPECTED VALUE IN INPUT WORDS 11 OR 12 (BITS 7-1)</u>
1	%0000001	%0000001
1C	%1111110	%1111110
2	%0000010	%0000010
2C	%1111101	%1111101
3	%0000100	%0000100
3C	%1111011	%1111011
4	%0001000	%0001000
4C	%1110111	%1110111
5	%0010000	%0010000
5C	%1101111	%1101111
6	%0100000	%0100000
6C	%1011111	%1011111
7	%1000000	%1000000
7C	%0111111	%0111111

3.2.3:2.3.5:8 IE Range Counter Test

The purpose of this test is to verify that each bit of both IE Range Counters can be toggled.

[IR675:1386;34] This test shall be performed by both DCU A and DCU B.

[IR675:591;109] The requirement of 3.2.3:2.3.5 (k) to verify the loaded content of the IE Range Counter shall be superseded by the steps of this test.

[IR675:1386;35] The IE Range Counter test shall be accomplished by writing then reading a rotating bit pattern, as shown in the following table, through the in-channel IE Range Counter (see Table XXXVII). [IR675:591;111] Failure to read the expected input pattern shall constitute failure of this test.

<u>PATTERN</u>	<u>OUTPUT TO IE RANGE COUNTER (BITS 6-0)</u>	<u>EXPECTED VALUE IN INPUT WORDS 11 OR 12 (BITS 14-8)</u>
1 1C	%0000001 %11111110	%0000001 %11111110
2 2C	%0000010 %11111101	%0000010 %11111101
3 3C	%0000100 %11111011	%0000100 %11111011
4 4C	%0001000 %11101111	%0001000 %11101111
5 5C	%0010000 %11011111	%0010000 %11011111
6 6C	%0100000 %10111111	%0100000 %10111111
7 7C	%1000000 %01111111	%1000000 %01111111

3.2.3:2.3.5:9 IE Terminate Sequence Test

The purpose of this test is to verify that an IE input sequence in progress can be terminated under software control by the in-control DCU.

[IR675:591;113] During the performance of this test, the requirement of 3.2.3:2.3.5 (k) to verify final state values for the IE Address Counter, IE Range Counter, and IE Channel Indicator shall not be performed. [IR675:591;114] The requirement to verify the state of the Conversion Complete indicator shall be superseded by the steps of this test.

[IR675:1430;2] This test shall be performed by both DCU A and DCU B, each while operating as the in-control DCU. For the in-control DCU, WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running.

(a) The test is conducted as follows:

- (1) [IR675:591;115] Bit patterns shall be stored into IE DPM locations TW1A through TW5B (Group 0) that are complementary to the patterns that are expected to be input during an IE input sequence (see Table XXX).
- (2) [IR675:591;116] A complete IE input sequence shall be initiated.
- (3) [IR675:591;117] The DCU shall delay 5.0 +5/-0 usec from initiation of the IE input sequence and then verify that the in-channel IE Conversion Complete indicator (Table XXXVII) indicates input not complete. [IR675:591;118] Failure to verify this status shall constitute test failure.
- (4) [IR675:591;119] At 175 +10/-10 usec from initiation of the IE input sequence, the Terminate IE Sequence I/O instruction shall be executed.
- (5) [IR675:591;120] The DCU shall delay 10 +5/-0 usec from execution of the instruction of step 4 and verify that the in-channel IE Conversion Complete indicator indicates that the input is complete. [IR675:591;121] Failure to verify this status shall constitute test failure.

3.2.3:2.3.5:9 IE Terminate Sequence Test (Continued)

- (6) [IR675:591;122] It shall be verified that IE DPM locations TW1A through TW2B contain bit patterns expected as a result of the input.  
[IR675:591;123] The DCU shall verify that locations TW4A/TW4B/TW5A/TW5B contain bit patterns as stored in step 1. [IR675:591;124] Failure of these locations to contain the proper values shall constitute failure of this test.

3.2.3:2.3.5:10 IE Pulse Rate Converter Control Bit Test

This test verifies that the PRC Overflow Test is not activated if the Start PRC Overflow Test on Channel A is commanded Off and the Start PRC Overflow Test on Channel B is commanded On. Further the test verifies that the PRC Overflow Test is not activated if the Start PRC Overflow Test on Channel A is commanded On and the Start PRC Overflow Test on Channel B is commanded Off.

[IR675:1430;3] This test shall be performed by DCU A while operating as the in-control DCU. WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running.

(a) Test steps are as follows:

- (1) [IR675:591;126] The test pattern \$5555 shall be written into IE DPM PRC locations N1, N2A/N2B, N3, Q1A1/Q1B1, and Q1A2/Q1B2 (see Table XXX).
- (2) [IR675:591;127] Start PRC Overflow Test on Channel A shall be commanded Off; and Start PRC Overflow Test on Channel B shall be commanded On (see Table XXXI).
- (3) [IR675:4597;11] After a delay of at least 135 msec, the IE input sequence for address locations \$820160 through \$82017A shall be initiated.
- (4) [IR675:4597;12] After a delay of at least 400 usec to allow for completion of the requested input, it shall be verified that both PRC Overflow Test indicators on Channel A and B (see Table XXXVII) indicate Off; and that the test pattern locations of step 1 have not been altered.

3.2.3:2.3.5:10 IE Pulse Rate Converter Control Bit Test  
(Continued)

- (5) [IR675:5070;1] Start PRC Overflow Test on Channel B shall be commanded Off; and Start PRC Overflow Test on Channel A shall be commanded On.
- (6) [IR675:4597;13] After a delay of at least 135 msec, the IE input sequence for address locations \$820160 through \$82017A shall be initiated.
- (7) [IR675:4597;14] After a delay of at least 400 usec to allow for completion of the requested input, it shall be verified that both PRC Overflow Test indicators on Channel A and B indicate Off; and that the test pattern locations of step 1 have not been altered.
- (8) [IR675:591;133] Start PRC Overflow Test on Channel A shall be commanded Off.

[IR675:591;134] If any of the conditions listed are not satisfied, a test failure shall be declared.

3.2.3:2.3.5:11 IE Pulse Rate Converter Test

The Pulse Rate Converter test verifies that the PRCs are capable of outputting bit patterns of both polarities onto the IE data bus and the correct control bits to the IE Sequencer. The test is performed by commanding Start PRC Overflow Test on for both Channel A and Channel B. This forces the PRC data alternately to all ones (\$FFFF) and all zeros (\$0000) depending on the state of the PRC toggle bit (MSB).

[IR675:1430;4] This test shall be performed by DCU A while operating as the in-control DCU. WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running.

[IR675:591;136] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

3.2.3:2.3.5:11 IE Pulse Rate Converter Test (Continued)

(a) The test sequence is specified below:

- (1) The OE A and OE B 2khz Excitation power supplies are in the Off state because of the initialization to this test by 3.2.3:2.3.5(c).
- (2) [IR675:4597;15] A test pattern other than \$FFFF or \$0000 shall be written into the IE DPM PRC locations N1, N2A/N2B, N3, TRCA/TRCB, Q1A1/Q1B1 and Q1A2/Q1B2 (see Table XXX).
- (3) [IR675:591;137] Start PRC Overflow Test on Channel A and Start PRC Overflow Test on Channel B shall be commanded On (see Table XXXI).
- (4) [IR675:2168;5] A delay of at least 20 msec and no more than 25 msec shall be allowed.
- (5) [IR675:4597;16] The input of address locations \$820160 through \$82017A shall be initiated.
- (6) [IR675:2168;7] A delay of at least 400 usec shall be allowed for IE input sequence completion.
- (7) [IR675:4597;17] IE DPM PRC locations of step 2 shall be verified to contain the test pattern written in step 2.
- (8) [IR675:2168;9] A delay of at least 135 msec from completion of step 3 shall be allowed for the first PRC counter overflow.
- (9) [IR675:4597;18] The input of address locations \$820160 through \$82017A shall be initiated.
- (10) [IR675:2168;10] A delay of at least 400 usec shall be allowed for IE input sequence completion.
- (11) [IR675:4597;19] IE DPM PRC locations of step 2 shall be verified to be either \$0000 or \$FFFF.

3.2.3:2.3.5:11 IE Pulse Rate Converter Test (Continued)

- (12) [IR675:2168;11] A delay of at least 135 msec shall be allowed for a second PRC counter overflow.
- (13) [IR675:4597;20] The input of address locations \$820160 through \$82017A shall be initiated.
- (14) [IR675:2168;12] A delay of at least 400 usec shall be allowed for IE input sequence completion.
- (15) [IR675:4597;21] IE DPM PRC locations of step 2 shall be verified to be the one's complement of the data from the first PRC overflow.
- (16) [IR675:2168;13] A delay of at least 135 msec shall be allowed for a third PRC counter overflow.
- (17) [IR675:4597;22] The input of address locations \$820160 through \$82017A shall be initiated.
- (18) [IR675:2168;14] A delay of at least 400 usec shall be allowed for IE input sequence completion.
- (19) [IR675:4597;23] IE DPM PRC locations of step 2 shall be verified to be the one's complement of the data from the second PRC overflow.
- (20) [IR675:2168;15] A delay of at least 135 msec shall be allowed for a fourth PRC counter overflow.
- (21) [IR675:591;154] Start PRC Overflow Test Channel A and Start PRC Overflow Test Channel B shall be commanded Off.
- (22) [IR675:4597;24] The input of address locations \$820160 through \$82017A shall be initiated.
- (23) [IR675:2168;16] A delay of at least 400 usec shall be allowed for IE input sequence completion.



3.2.3:2.3.5:11 IE Pulse Rate Converter Test (Continued)

- (24) [IR675:4597;25] IE DPM PRC locations of step 2 shall be verified to be the one's complement of the data from the third PRC overflow.
- (25) [IR675:4597;26] A test pattern other than \$FFFF or \$0000 shall be written into the IE DPM PRC locations of step 2.
- (26) [IR675:2168;17] An additional delay of at least 135 msec shall be allowed from issuance of commands to turn the overflow off (step 21).
- (27) [IR675:4597;27] The input of address locations \$820160 through \$82017A shall be initiated.
- (28) [IR675:2168;18] A delay of at least 400 usec shall be allowed for IE input sequence completion.
- (29) [IR675:4597;28] IE DPM PRC locations of step 2 shall be verified to contain the test pattern written in step 25.

3.2.3:2.3.5:12 OE Storage Registers Test

The OE Storage Registers test verifies that the OE Storage Registers are functional and that they are capable of storing and outputting all bit patterns. The test also verifies that the data bus and address bus are functional.

[IR675:1430;5] This test shall be performed by both DCU A and DCU B each while operating as the in-control DCU. For the in-control DCU, WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running.

[IR675:591;165] During the performance of this test, the requirement of 3.2.3:2.3.5(i) to read the contents of the OE Storage Register prior to its transfer shall be superseded by the steps of this procedure.

[IR675:1386;37] The test shall be accomplished by writing a rotating bit pattern of both polarities, per the following table, to the storage register in OE A and the storage register in OE B. [IR675:591;167] The test shall then verify the bit pattern by reading back the contents of each storage register (See Table XXXVII).

3.2.3:2.3.5:12 OE Storage Registers Test (Continued)

[IR675:591;168] Failure to read back the same value as was loaded shall constitute a failure of the test.

<u>NUMBER</u>	<u>OE STORAGE REGISTER TEST PATTERNS</u>	<u>NUMBER</u>	<u>OE STORAGE REGISTER TEST PATTERNS</u>
1	\$0001	9	\$0100
1C	\$FFFE	9C	\$FEFF
2	\$0002	10	\$0200
2C	\$FFFD	10C	\$FDEF
3	\$0004	11	\$0400
3C	\$FFFB	11C	\$FBFF
4	\$0008	12	\$0800
4C	\$FFF7	12C	\$F7FF
5	\$0010	13	\$1000
5C	\$FFEF	13C	\$EFFF
6	\$0020	14	\$2000
6C	\$FFDF	14C	\$DFFF
7	\$0040	15	\$4000
7C	\$FFBF	15C	\$BFFF
8	\$0080	16	\$8000
8C	\$FF7F	16C	\$7FFF

3.2.3:2.3.5:13 D/A and A/D Converter Wraparound Test

The intent of this test was to verify the linearity and resolution of each D/A converter in the OEs, and the A/D converter in each IE. Because of system noise combined with the lack of resolution from the D/A and A/D converters, the test could not resolve the three least significant bits properly. Adequate checks are provided by the IE Analog to Digital Converter Self-Test of 3.2.3:3.3.3 and the OE Digital to Analog Converters Self-Test of 3.2.3:3.3.5.

3.2.3:2.3.5:14 Watchdog Timer Counter/Time Reference Interrupt Test

The purpose of this test is to verify WDT time-out period by means of the Real Time Clock, generation of WDTs, RCFIs, TRI enable/disable, and pending operations.

Performance of this test will require the coordination of DCU A and DCU B as outlined.

[IR675:591;191] During the performance of this test, normal WDT1, WDT2, RCFI1, RCFI2, and TRI processing shall be suspended. The processing of these interrupts during this test are specified within the steps of this test.

[IR675:591;192] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

TEST SUMMARY:

The test demonstrates that:

- (a) By use of the Real Time Clock, the time period between resetting the WDTs and WDT time-out is  $18 \pm 3$  msec.
- (b) Both WDT interrupts are serviced between 15 msec and 21 msec after resetting the WDTs.
- (c) Both RCFIs are serviced within 21 msec after resetting the cross-channel DCU's WDTs.
- (d) Once the TRI is enabled and the interrupt is pending, a TRI will be serviced before the execution of the third instruction after the enabling of the TRI.

3.2.3:2.3.5:14 Watchdog Timer Counter/Time Reference  
Interrupt Test (Continued)

The test is conducted as follows:

- | DCU A  | DCU B  |
|--|--|
| 1. [IR675:591;193] Both WDTs shall be reset.   | 1. [IR675:591;194] This DCU B test sequence shall commence upon completion of DCU A test sequence step 3.    |
| 2. [IR675:591;195] TRI shall be cleared and enabled.   |  |
| 3. [IR675:591;196] Both WDTs shall be reset and both WDTH interrupts cleared and enabled for each occurrence of a TRI.   |  |
| 4. [IR675:591;197] This DCU A test sequence shall continue after completion of DCU B test sequence step 3.   |  |
|  | 2. [IR675:591;198] Both WDTs shall be continually reset.   |
|  | 3. [IR675:591;199] TRI, RCFI1, and RCFI2 shall be cleared and enabled.                                       |
|  | 4. [IR675:4102;2] This DCU B test sequence shall continue upon notification from DCU A test sequence step 6. |
| 5. [IR675:4381;4] On the next occurrence of a TRI indication, both WDTs shall be reset, the RTC Output shall be saved, and the TRI shall be disabled in the CIE. |  |
| 6. [IR675:591;202] DCU B shall be notified of the time of the TRI occurrence.  |  |

3.2.3:2.3.5:14 Watchdog Timer Counter/Time Reference  
Interrupt Test (Continued)

5. [IR675:4102;4] Both RCFI1 and RCFI2 shall be verified to be serviced within 21 msec of DCU A's notification of last resetting of its WDTs.  
[IR675:1386;47] The RTC Output adjusted for RTC rollover shall be used to verify the above elapsed time from the last resetting of DCU A's WDTs.
7. [IR675:591;203] Both WDTs shall be verified to be in the non-timed-out state through use of the WDT1/WDT2 Timed-Out Status word (See Table XXXVII).
8. [IR675:1386;44] Both WDT1 and WDT2 shall be verified to be serviced no sooner than 15 msec and no longer than 21 msec from the resetting of the WDTs.  
[IR675:1386;45] The RTC Output adjusted for RTC rollover shall be used to verify the above elapsed times from the resetting of the WDTs.
9. [IR675:591;205] The corresponding WDT1/WDT2 Timed-Out Status shall be verified to indicate that the corresponding WDTs are in the timed-out state.
10. [IR675:591;207] This DCU A test sequence shall continue upon completion of DCU B test sequence step 5.

3.2.3:2.3.5:14 Watchdog Timer Counter/Time Reference  
Interrupt Test (Continued)

11. [IR675:591;208] Both WDTs shall be reset.
12. [IR675:1386;48] Both WDT1 and WDT2 shall be cleared.
13. [IR675:1386;49] The TRI shall be verified not pending (See Table XXXVII).
14. [IR675:1386;50] The TRI shall be enabled in the CIE.
15. [IR675:591;212] The TRI shall be verified to be serviced before the execution of the third instruction after the instruction that enables the TRI.
16. [IR675:1386;51] The TRI shall be verified to be pending.

[IR675:591;214] Upon completion of these steps, both DCUs shall be reinitialized to the prerequisite test conditions specified in 3.2.3:2.3.5(c).

[IR675:591;215] The above steps shall be executed again with DCU B performing the steps shown for DCU A, and DCU A performing the steps shown for DCU B (changing any DCU references to that of the cross-channel DCU).

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test

The Watchdog Timer Interrupt test verifies that a timed-out WDT will generate a WDTI interrupt to the in-channel DCU and an RCFI to the cross-channel DCU, and verifies the operation of the WDTI and RCFI CIE interrupt mask register and pending status bits.

Performance of this test will require the coordination of DCU A and DCU B as outlined. The steps listed below specify an ordering of events with respect to processing.

The test is accomplished by setting each WDT in each channel to the timed-out state and verifying the generation of the interrupts. [IR675:591;216] During the performance of this test normal WDTI1, WDTI2, RCFI1 and RCFI2 processing shall be inhibited. The processing of these interrupts during this test is specified within the steps of this test.

[IR675:591;217] Any result other than that which is specified in the test sequence steps below shall constitute a test failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

TEST SUMMARY:

The test demonstrates that:

- (a) No DCU A WDTI1 interrupt will be pending while it is disabled in the CIE, and conversely that it will be serviced (and WDTI2 will not be) while it is enabled in the CIE.
- (b) No DCU B RCFI1 interrupt and no DCU B WDTI1 interrupt will be pending while they are disabled in the CIE, and conversely that they will be serviced (and RCFI2 and WDTI2 will not be) while they are enabled in the CIE.
- (c) No DCU A RCFI1 interrupt and no DCU A WDTI2 interrupt will be pending while they are disabled in the CIE, and conversely that they will be serviced (and RCFI2 and WDTI1 will not be) while they are enabled in the CIE.
- (d) No DCU B RCFI2 interrupt and no DCU B WDTI2 interrupt will be pending while they are disabled in the CIE, and conversely that they will be serviced (and RCFI1 and WDTI1 will not be) while they are enabled in the CIE.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

- (e) No DCU A RCFI2 interrupt will be pending while it is disabled in the CIE, and conversely that it will be serviced (and RCFI1 will not be) while it is enabled in the CIE.

The test is conducted as follows:

- | DCU A  | DCU B  |
|--|--|
| 1. [IR675:591;218] The interrupt level shall be set to 4.  | 1. [IR675:591;219] This DCU B test sequence shall commence upon completion of DCU A test sequence step 2.  |
| 2. [IR675:591;220] The WDTs shall be continually reset during the remainder of this test unless specified otherwise (since TRIs will not occur, the program must periodically reset the WDTs so that unexpected time-outs will not occur). |  |
| 3. [IR675:591;221] This DCU A test sequence shall continue upon completion of DCU B test sequence step 4.  |  |
|  | 2. [IR675:1386;52] The interrupt level shall be set to 4.  |
|  | 3. [IR675:591;222] The WDTs shall be continually reset during the remainder of this test unless specified otherwise (since TRIs will not occur, the program must periodically reset the WDTs so that unexpected time-outs will not occur). |
|  | 4. [IR675:1386;53] WDTH1, WDTH2, RCFI1, AND RCFI2 shall be disabled and cleared in the CIE.  |



3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

5. [IR675:591;224] This DCU B test sequence shall continue upon completion of DCU A test sequence step 11.
4. [IR675:1386;54] WDT1, WDT2, RCFI1, and RCFI2 shall be disabled and cleared in the CIE.
5. [IR675:4381;5] WDT1 shall be set to the timed-out state, and then continually reset after at least a 5.5 usec delay.
6. [IR675:591;227] The non-pending status of WDT1 shall be verified (See Table XXXVII).
7. [IR675:591;228] WDT1 shall be enabled in the CIE.
8. [IR675:591;229] The non-pending status of WDT2 and the pending status of WDT1 shall be verified.
9. [IR675:1386;55] The interrupt level shall be set to 0 then set to 4.
10. [IR675:591;240] WDT1 shall be verified to be serviced.
11. [IR675:1386;56] WDT1 shall be disabled and cleared in the CIE.
12. [IR675:591;242] This DCU A test sequence shall continue upon completion of DCU B test sequence step 17.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

6. [IR675:591;243] RCFI1 shall be verified to be non-pending (See Table XXXVII).
7. [IR675:591;244] RCFI1 shall be enabled in the CIE.
8. [IR675:591;245] RCFI1 shall be verified to be pending and RCFI2 not pending.
9. [IR675:1386;57] The interrupt level shall be set to 0, then to 4.
10. [IR675:1386;58] RCFI1 shall be verified to be serviced.
11. [IR675:4381;6] WDT1 shall be set to the timed-out state, and then continually reset after at least a 5.5 usec delay.
12. [IR675:591;247] WDT1 shall be verified to be non-pending.
13. [IR675:1386;59] RCFI1 shall be disabled and cleared and WDT1 enabled in the CIE.
14. [IR675:591;249] WDT1 shall be verified to be pending and WDT2 not pending.
15. [IR675:591;250] The interrupt level shall be set to 0 and then to 4.
16. [IR675:591;251] WDT1 shall be verified to be serviced.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

17. [IR675:1386;60] WDT1 shall be disabled and cleared in the CIE.
18. [IR675:591;253] This DCU B test sequence shall continue upon completion of DCU A test sequence step 25.
13. [IR675:591;254] RCFI1 shall be verified to be not pending.
14. [IR675:591;255] RCFI1 shall be enabled in the CIE.
15. [IR675:591;256] RCFI1 shall be verified to be pending and RCFI2 not pending.
16. [IR675:591;257] The interrupt level shall be set to 0, then to 4.
17. [IR675:591;258] RCFI1 shall be verified to be serviced.
18. [IR675:1386;61] RCFI1 shall be disabled and cleared in the CIE.
19. [IR675:4381;7] WDT2 shall be set to the timed-out state, and then continually reset after at least a 5.5 usec delay.
20. [IR675:591;261] WDT2 shall be verified to be non-pending.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

21. [IR675:591;262] WDTM2 shall be enabled in the CIE.
  22. [IR675:591;263] WDTM2 shall be verified to be pending and WDTM1 not pending.
  23. [IR675:591;264] The interrupt level shall be set to 0, and then to 4.
  24. [IR675:591;265] WDTM2 shall be verified to be serviced.
  25. [IR675:1386;63] WDTM2 shall be disabled and cleared in the CIE.
  26. [IR675:591;267] This DCU A test sequence shall continue upon completion of DCU B test sequence step 30.
- 
19. [IR675:591;268] RCFI2 shall be verified to be not pending.
  20. [IR675:591;269] RCFI2 shall be enabled in the CIE.
  21. [IR675:591;270] RCFI2 shall be verified to be pending and RCFI1 not pending.
  22. [IR675:591;271] The interrupt level shall be set to 0, then to 4.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

23. [IR675:591;272] RCFI2 shall be verified to be serviced.
  24. [IR675:4381;8] WDT2 shall be set to the timed-out state, and then continually reset after at least a 5.5 usec delay.
  25. [IR675:591;274] WDTH2 shall be verified to be non-pending.
  26. [IR675:1386;64] RCFI2 shall be disabled and cleared and WDTH2 enabled in the CIE.
  27. [IR675:591;276] WDTH2 shall be verified to be pending and WDTH1 not pending.
  28. [IR675:591;277] The interrupt level shall be set to 0 and then to 4.
  29. [IR675:591;278] WDTH2 shall be verified to be serviced.
  30. [IR675:1386;65] WDTH2 shall be disabled and cleared in the CIE.
- 
27. [IR675:591;280] RCFI2 shall be verified to be non-pending.
  28. [IR675:591;281] RCFI2 shall be enabled in the CIE.
  29. [IR675:591;282] RCFI2 shall be verified to be pending and RCFI1 not pending.

3.2.3:2.3.5:15 Watchdog Timer Interrupt Test (Continued)

30. [IR675:591;283] The interrupt level shall be set to 0, then to 4.
31. [IR675:591;284] RCFI2 shall be verified to be serviced.
32. [IR675:1386;66] RCFI2 shall be disabled and cleared in the CIE.

3.2.3:2.3.5:16 Watchdog Timer OE Data Switch Test

The Watchdog Timer OE Data Switch Test verifies that only DCU A can control the OEs when both of its WDTs are in the non-timed-out state, and that only DCU B can control the OEs when either of DCU A's WDTs is in the timed-out-state.

Performance of this test will require the coordination of DCU A and DCU B as outlined. The steps listed below specify an ordering of events with respect to processing.

[IR675:591;286] During the performance of this test, the requirement of 3.2.3:2.3.5(i) to read the value stored in the OE storage register shall be superseded by the steps of this test.

[IR675:1386;67] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

The test is conducted as follows:

- | DCU A  | DCU B  |
|--|--|
| 1. [IR675:1386;68] The WDTs shall be continually reset during this test unless specified otherwise.                        | 1. [IR675:1386;69] This DCU B test sequence shall commence upon completion of DCU A test sequence step 2.            |
| 2. [IR675:1386;70] Channel A and Channel B OE Storage Registers shall be loaded and verified with the test pattern \$0F0F. |  |
| 3. [IR675:1386;71] This DCU A test sequence shall continue upon completion of DCU B test sequence step 3.                  | 2. [IR675:1386;72] The WDTs shall be continually reset during the remainder of this test unless specified otherwise. |

3.2.3:2.3.5:16 Watchdog Timer OE Data Switch Test  
(Continued)

3. [IR675:1386;73] Channel A and Channel B OE Storage Registers shall be loaded with the test pattern \$F0F0.
4. [IR675:1386;74] This DCU B test sequence shall continue upon completion of DCU A test sequence step 6.
4. [IR675:1386;75] Channel A and Channel B OE Storage Registers shall be verified as retaining the test pattern \$0F0F.
5. [IR675:1386;76] WDT1 shall be commanded to the timed-out state, while continually resetting WDT2.
6. [IR675:1386;77] Channel A and Channel B OE Storage Registers shall be loaded with the test pattern \$0000 and verified that the registers retain the test pattern \$0F0F.
7. [IR675:1386;78] This DCU A test sequence shall continue upon completion of DCU B test sequence step 5.
5. [IR675:1386;79] Channel A and Channel B OE Storage Registers shall be loaded with the test pattern \$F0F0.
6. [IR675:1386;80] This DCU B test sequence shall continue upon completion of DCU A test sequence step 10.



3.2.3:2.3.5:16 Watchdog Timer OE Data Switch Test  
(Continued)

8. [IR675:1386;81] Channel A and Channel B OE Storage Registers shall be verified to contain the test pattern \$F0F0.
9. [IR675:1386;82] WDT1 shall be continually reset, while WDT2 shall be commanded to the timed-out state.
10. [IR675:1386;83] Channel A and Channel B OE Storage Registers shall be loaded with the test pattern \$FFFF and verified that the registers retain the test pattern \$F0F0.
11. [IR675:1386;84] This DCU A test sequence shall continue upon completion of DCU B test sequence step 7.
7. [IR675:1386;85] Channel A and Channel B OE Storage Registers shall be loaded with the test pattern \$0F0F.
12. [IR675:1386;86] Channel A and Channel B OE Storage Registers shall be verified to contain the test pattern \$0F0F.

3.2.3:2.3.5:17 Watchdog Timer IE Data Switch Test

The Watchdog Timer IE Data Switch test verifies that DCU A is prevented from initiating an IE input sequence when either of its WDTs is in the timed-out state, and that DCU B is prevented from initiating an IE input sequence when both DCU A's WDTs are in the non-timed-out state.

Performance of this test will require coordination of DCU A and DCU B as outlined. The steps listed below specify an ordering of events with respect to processing.

[IR675:2168;19] During the performance of this test, the requirement of 3.2.3:2.3.5(k) to verify the final state of the IE Address and Range Counters and the IE Channel Indicator upon expected completion of the IE input sequence shall not be performed.

[IR675:2168;20] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

The test is conducted as follows:

- | DCU A  | DCU B   |
|--|---|
| 1. [IR675:2168;21] The WDTs shall be continually reset during this test unless specified otherwise.  | 1. [IR675:2168;22] The WDTs shall be continually reset during this test unless specified otherwise.       |
| 2. [IR675:2168;23] IE DPM locations TW1A and TW1B shall be set to zero.                              | 2. [IR675:4697;4] This DCU B test sequence shall continue upon completion of DCU A test sequence step 11. |
| 3. [IR675:2168;25] WDT1 shall be commanded to the timed-out state, while continually resetting WDT2. |   |
| 4. [IR675:2168;26] An IE input sequence shall be initiated in an attempt to input TW1A and TW1B.     |   |
| 5. [IR675:2168;27] A delay of at least 200 usec shall be allowed.                                    |   |

3.2.3:2.3.5:17 Watchdog Timer IE Data Switch Test (Continued)

6. [IR675:2168;28] TW1A and TW1B shall be verified as retaining the value of zero.
7. [IR675:2168;29] WDT1 shall be continually reset, while WDT2 shall be commanded to the timed-out state.
8. [IR675:2168;30] An IE input sequence shall be initiated in an attempt to input TW1A and TW1B.
9. [IR675:2168;31] A delay of at least 200 usec shall be allowed.
10. [IR675:2168;32] TW1A and TW1B shall be verified as retaining the value of zero.
11. [IR675:2168;33] WDT2 shall be continually reset.
12. [IR675:2168;34] This DCU A test sequence shall continue upon completion of DCU B test sequence step 3.
3. [IR675:2168;35] An IE input sequence shall be initiated in an attempt to input TW1A and TW1B.
13. [IR675:2168;36] A delay of at least 200 usec shall be allowed.
14. [IR675:2168;37] TW1A and TW1B shall be verified as retaining the value of zero.

3.2.3:2.3.5:18 Watchdog Timer VRC Data Switch Test

The Watchdog Timer VRC Data Switch test verifies that DCU A is prevented from initiating VRC transmission when either of its WDTs is in the timed-out state, and that DCU B is prevented from initiating VRC transmission when both DCU A's WDTs are in the non-timed-out state.

Performance of this test will require the coordination of DCU A and DCU B as outlined. The steps listed below specify an ordering of events with respect to processing.

[IR675:2168;38] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

The test is conducted as follows:

- | DCU A   | DCU B  |
|---|--|
| 1. [IR675:2168;39] The WDTs shall be continually reset during this test unless specified otherwise.   | 1. [IR675:2168;40] The WDTs shall be continually reset during this test unless specified otherwise.        |
| 2. [IR675:2168;41] WDT1 shall be commanded to the timed-out state, while continually resetting WDT2.  | 2. [IR675:2168;42] This DCU B test sequence shall continue upon completion of DCU A test sequence step 10. |
| 3. [IR675:2168;43] A VRC transmission shall be initiated in an attempt to output to the VRC.  |  |
| 4. [IR675:2168;44] A $40 \pm 10$ usec delay shall be allowed.   |  |
| 5. [IR675:2168;45] VRCA-VDT1A and VRCA-VDT2A address registers and corresponding complete indicators shall be verified as remaining in the complete state, i.e., address registers are zero; complete bits are 1. (See Table XXXVII). |  |

3.2.3:2.3.5:18 Watchdog Timer VRC Data Switch Test  
(Continued)

6. [IR675:2168;46] WDT1 shall be continually reset, while WDT2 shall be commanded to the timed-out state.
  7. [IR675:2168;47] A VRC transmission shall be initiated in an attempt to output to the VRC.
  8. [IR675:2168;48] A  $40 \pm 10$  usec delay shall be allowed.
  9. [IR675:2168;49] VRCA-VDT1A and VRCB-VDT2A address registers and corresponding complete indicators shall be verified as remaining in the complete state.
  10. [IR675:2168;50] WDT2 shall be continually reset.
3. [IR675:2168;51] A VRC transmission shall be initiated in an attempt to output to the VRC.
  4. [IR675:2168;52] A  $40 \pm 10$  usec delay shall be allowed.
  5. [IR675:2168;53] VRCA-VDT1B and VRCB-VDT2B address registers and corresponding complete indicators shall be verified as remaining in the complete state.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test

The purpose of the test is to assure that the OE Power Safety Switch can be controlled by the in-control DCU. The steps below specify an ordering of events with respect to processing.

[IR675:5415;1] All verifications of power supply states shall be made within the tolerances indicated in Table XXXIV.

[IR675:591;314] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

## TEST SUMMARY:

The sequence of steps needed to turn on (off) a power supply and to verify that it is turned on (off) are:

- (a) Issue the "Turn On (Off) OE A Power Control Switch" and "Turn On (Off) OE B Power Control Switch" I/O instructions.
- (b) Delay 100 +/-10 usec to allow the bits to flip, then verify that the appropriate OE Power Safety Switches are On (Off).
- (c) Turn on (off) the OE A and OE B 2khz RVDT/LVDT power supplies and vary the source of excitation.
- (d) Energize the Fuel System Purge Solenoids to the Pull-In level, energize the CCV fail-safe servoswitches to provide a load to power supplies.
- (e) Delay 110 +/-10 msec to allow the solenoid and servoswitch power supplies to stabilize.
- (f) Check that the power supplies are turned on (off) by verifying that the dual port memory inputs are within the ranges established for an "On" (Off") condition of the power supplies.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

This test demonstrates that:

- (g) DCU A can turn on (and DCU B cannot turn off), then turn off (and DCU B cannot turn on) the OE power supplies when DCU A's watchdog timers are reset (not timed-out).
- (h) DCU B can turn on (and DCU A cannot turn off), then turn off (and DCU A cannot turn on) the OE power supplies when either of DCU A's watchdog timers is timed-out.

Test sequence is as follows:

- | DCU A  | DCU B  |
|--|--|
| 1. [IR675:591;317] WDT1 and WDT2 shall be continually reset.   | 1. [IR675:591;318] WDT1 and WDT2 shall be continually reset.   |
| 2. [IR675:591;319] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued. | 2. [IR675:591;320] This DCU B test sequence shall continue upon completion of DCU A test sequence step 11. |
| 3. [IR675:591;321] A 100 +/- 10 usec delay shall be allowed.   |  |
| 4. [IR675:591;322] The OE A Power Safety Switch (Input Word 15) shall be verified to be On.                                      |  |
| 5. [IR675:591;323] The OE B Power Safety Switch (Input Word 16) shall be verified to be On.                                      |  |
| 6. [IR675:591;324] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel A.        |  |

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

7. [IR675:1386;90] Both Fuel System Purge solenoids shall be energized to the Pull-In level.
8. [IR675:591;326] Both CCV fail-safe servoswitches shall be energized.
9. [IR675:591;327] A 110 +/- 10 msec delay shall be allowed following issuance of the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.
10. [IR675:591;328] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, and FRVA/FRVB power supply outputs shall be verified to be On.
11. [IR675:1843;1] SL1/SL2 power supply outputs shall be verified to be at the Pull-In level.
12. [IR675:1386;92] This DCU A test sequence shall continue upon completion of DCU B test sequence step 3.
3. [IR675:591;330] "Turn Off OE A Power Control Switch" and "Turn Off OE B Power Control Switch" I/O instructions shall be issued.
4. [IR675:591;331] This DCU B test sequence shall continue upon completion of DCU A test sequence step 24.



3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

13. [IR675:591;332] 100 +/-10 usec after step 3 of DCU B test sequence is completed, OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.
14. [IR675:591;333] A 110 +/-10 msec delay shall be allowed.
15. [IR675:591;334] OE1A/OE1B, OE2A/OE2B, OE7A/OE7B and FRVA/FRVB power supply outputs shall be verified to be On.
16. [IR675:1386;93] The SL1/SL2 power supply outputs shall be verified to be at the Pull-In level.
17. [IR675:591;336] "Turn Off OE A Power Control Switch" and "Turn Off OE B Power Control Switch" I/O instructions shall be issued.
18. [IR675:591;337] A 100 +/-10 usec delay shall be allowed.
19. [IR675:591;338] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
20. [IR675:1386;94] A 48 +/-1 msec delay shall be allowed.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

21. [IR675:1386;95] OE1A/OE1B, OE7A/OE7B, SL1/SL2, and FRVA/FRVB power supply outputs shall be verified to be Off.
  22. [IR675:5150;2] All On/Off devices affected by the turning off of the OE A and OE B Power Control Switches shall be verified to be deactivated. These On/Off devices include all solenoids excluding spares, all fail-operational and fail-safe servoswitches excluding spares, and the igniters.
  23. [IR675:1386;96] A 23 +/-1 msec delay shall be allowed.
  24. [IR675:1386;97] OE2A/OE2B power supply outputs shall be verified to be Off.
  25. [IR675:1386;98] This DCU A test sequence shall continue upon completion of DCU B test sequence step 5.
- 
5. [IR675:591;342] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued.
  6. [IR675:591;343] This DCU B test sequence shall continue upon completion of DCU A test sequence step 31.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

26. [IR675:591;344] 100 +/-10 usec after step 5 of DCU B test sequence is completed, OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
  27. [IR675:1386;99] The resetting of WDT1 shall be discontinued.
  28. [IR675:591;346] This test sequence shall continue 25 +/-3 msec after the last Reset WDT1 I/O instruction.
  29. [IR675:591;347] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued.
  30. [IR675:591;348] A 100 +/-10 usec delay shall be allowed.
  31. [IR675:591;349] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
  32. [IR675:591;350] This DCU A test sequence shall continue upon completion of DCU B test sequence step 13.
7. [IR675:591;351] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued.
  8. [IR675:591;352] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel B.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

9. [IR675:5141;1] Both Fuel System Purge solenoids shall be energized to the Pull-In level. The expected energized state will be verified after the appropriate delay time as required by the Engine-Controller On/Off Devices monitoring of 3.2.3:2.3.5(j).

[IR675:5141;2] Both Fuel System Purge solenoids shall be commanded to the Hold level. Because the solenoids were energized when commanded to the Pull-In level, reverification of the energized state is not necessary for the Hold level.

10. [IR675:591;354] Both CCV fail-safe servoswitches shall be energized.

11. [IR675:1386;100] A 110 +/- 10 msec delay shall be allowed following issuance of the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.

12. [IR675:591;356] OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, and FRVA/FRVB power supply outputs shall be verified to be On.

13. [IR675:591;357] SL1/SL2 power supply outputs shall be verified to be at the Hold level.

14. [IR675:1462;2] This DCU B test sequence shall continue upon completion of DCU A test sequence step 35.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

33. [IR675:591;358] WDT1 shall be continually reset, while the resetting of WDT2 shall be discontinued.
  34. [IR675:591;359] A 25 +/-3 msec delay shall be allowed after the last Reset WDT2 command.
  35. [IR675:591;360] "Turn Off OE A Power Control Switch" and "Turn Off OE B Power Control Switch" I/O instructions shall be issued.
15. [IR675:591;362] 100 +/-10 usec after completing DCU A test sequence step 35, OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.
  16. [IR675:591;363] A 110 +/-10 msec delay shall be allowed.
  17. [IR675:591;364] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B and FRVA/FRVB power supply outputs shall be verified to be On.
  18. [IR675:591;365] The SL1/SL2 power supply outputs shall be verified to be set to the Hold level.
  19. [IR675:591;366] "Turn Off OE A Power Control Switch" and "Turn Off OE B Power Control Switch" I/O instructions shall be issued.

3.2.3:2.3.5:19 OE Power Safety Switch DCU Control Test  
(Continued)

20. [IR675:591;367] A 100 +/-10 usec delay shall be allowed.
21. [IR675:591;368] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
22. [IR675:1386;101] A 48 +/-1 msec delay shall be allowed.
23. [IR675:1386;102] OE1A/OE1B, SL1/SL2, and FRVA/FRVB power supply outputs shall be verified Off.
24. [IR675:5150;3] All devices affected by the turning off of the OE A and OE B Power Control Switches shall be verified to be deactivated. These On/Off devices include all solenoids excluding spares, all fail-operational and fail-safe servoswitches excluding spares, and the igniters.
25. [IR675:1386;103] A 23 +/-1 msec delay shall be allowed.
26. [IR675:1386;104] OE2A/OE2B power supply outputs shall be verified to be Off.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test

This test verifies that WDT control of the OE Power Safety Switch, the 2khz RVDT/LVDT power supply and the OE On/Off Registers is operating properly.

The steps below specify an ordering of events with respect to processing.

[IR675:5415;2] All verifications of power supply states shall be made within the tolerances indicated in Table XXXIV.

[IR675:591;373] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

TEST SUMMARY:

The sequence of steps needed to turn on (off) a power supply and to verify that it is turned on (off) are:

- (a) Issue the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.
- (b) Delay 100 +/-10 usec to allow the bits to flip, then verify that the appropriate OE Power Safety Switches are On (Off).
- (c) Turn on (off) the OE A and OE B 2khz RVDT/LVDT power supplies and vary the source of excitation.
- (d) Energize the Fuel System Purge Solenoids to the Pull-In level, energize the CCV fail-safe servoswitches to provide a load to power supplies.
- (e) Delay 110 +/-10 msec to allow the solenoid and servoswitch power supplies to stabilize.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

- (f) Check that the power supplies are turned on (off) by verifying that the dual port memory inputs are within the ranges established for an "On" (Off") condition of the power supplies.

This test demonstrates that:

- (g) DCU A can turn on the OE power supplies using Channel A excitation when both of its watchdog timers are reset, and subsequently that the electronics will shutdown the OE power supplies when DCU A WDT1 is timed-out and DCU B WDT2 is timed-out.
- (h) DCU A can turn on the OE power supplies using Channel B excitation when both of its watchdog timers are reset, and subsequently that the electronics will shutdown the OE power supplies when DCU A WDT2 is timed-out and DCU B WDT1 is timed-out.

The test sequence is as follows:

- | DCU A   | DCU B   |
|---|---|
| <p>1. [IR675:591;376] WDT1 and WDT2 shall be continually reset.</p>   | <p>1. [IR675:591;377] WDT1 and WDT2 shall be continually reset.</p> <p>2. [IR675:591;378] This DCU B test sequence shall continue upon completion of DCU A test sequence step 10.</p> |
| <p>2. [IR675:591;379] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued.</p> |   |
| <p>3. [IR675:591;380] A 100 +/-10 usec delay shall be allowed.</p>  |   |
| <p>4. [IR675:591;381] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.</p>                             |   |



3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

5. [IR675:591;382] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel A.

6. [IR675:5141;3] Both Fuel System Purge solenoids shall be energized to the Pull-In level. The expected energized state will be verified after the appropriate delay time as required by the Engine-Controller On/Off Devices monitoring of 3.2.3:2.3.5(j).

[IR675:5141;4] Both Fuel System Purge solenoids shall be commanded to the Hold level. Because the solenoids were energized when commanded to the Pull-In level, reverification of the energized state is not necessary for the Hold level.

7. [IR675:591;384] Both CCV fail-safe servoswitches shall be energized.

8. [IR675:591;385] A 110 +/-10 msec delay shall be allowed following issuance of the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.

9. [IR675:591;386] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, and FRVA/FRVB power supply outputs shall be verified to be On.

10. [IR675:591;387] The SL1/SL2 power supply outputs shall be verified to be at the Hold level.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

11. [IR675:1386;105] This DCU A test sequence shall continue upon completion of DCU B test sequence step 3.
3. [IR675:1386;106] The resetting of WDT2 shall be discontinued.
4. [IR675:4102;9] This DCU B test sequence shall continue upon completion of DCU A test sequence step 15.
12. [IR675:1386;107] After completion of DCU B test sequence step 3, the resetting of WDT1 shall be discontinued.
13. [IR675:591;391] A 25 +/-3 msec delay shall be allowed after the last Reset WDT1 I/O instruction.
14. [IR675:591;392] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
15. [IR675:591;393] A 110 +/-10 msec delay shall be allowed.
16. [IR675:4102;10] This DCU A test sequence shall continue upon completion of DCU B test sequence step 6.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

5. [IR675:4102;11] OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, SL1/SL2, and FRVA/FRVB power supply outputs shall be verified to be Off.
  6. [IR675:4102;12] All devices controlled by the OE A and OE B On/Off Registers shall be verified to be deactivated.
  7. [IR675:4102;13] This DCU B test sequence shall continue upon completion of DCU A test sequence step 26.
- 
17. [IR675:1386;108] WDT1 shall be continually reset.
  18. [IR675:591;397] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued.
  19. [IR675:591;398] A 100 +/-10 usec delay shall be allowed.
  20. [IR675:591;399] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.
  21. [IR675:591;400] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel B.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

22. [IR675:5141;5] Both Fuel System Purge Solenoids shall be energized to the Pull-In level. The expected energized state will be verified after the appropriate delay time as required by Engine-Controller On/Off Devices monitoring of 3.2.3:2.3.5(j).

[IR675:5141;6] Both Fuel System Purge solenoids shall be commanded to the Hold level. Because the solenoids were energized when commanded to the Pull-In level, reverification of the energized state is not necessary for the Hold level.

23. [IR675:591;402] Both CCV fail-safe servoswitches shall be energized.

24. [IR675:5150;4] A 110 +/-10 msec delay shall be allowed following issuance of the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.

25. [IR675:591;404] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, and FRVA/FRVB power supply outputs shall be verified to be On.

26. [IR675:591;405] The SL1/SL2 power supply outputs shall be verified to be at the Hold level.

27. [IR675:4102;14] This DCU A test sequence shall continue upon completion of DCU B test sequence step 8.

3.2.3:2.3.5:20 OE Power Safety Switch Power Down Matrix Test  
(Continued)

8. [IR675:591;406] WDT2 shall be continually reset and the resetting of WDT1 shall be discontinued.
9. [IR675:4102;15] This DCU B test sequence shall continue upon completion of DCU A test sequence step 31.
28. [IR675:4102;16] After completion of DCU B test sequence step 8, the resetting of WDT2 shall be discontinued.
29. [IR675:591;408] A 25 +/-3 msec delay shall be allowed.
30. [IR675:591;409] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be Off.
31. [IR675:591;410] A 110 +/-10 msec delay shall be allowed.
10. [IR675:4102;17] OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, SL1/SL2, and FRVA/FRVB power supply outputs shall be verified to be Off.
11. [IR675:4102;18] All devices controlled by the OE A and OE B On/Off Registers shall be verified to be deactivated.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power Up  
Reset Test

This test verifies OE voltage monitor control of the OE Power Safety Switch, the 2khz RVDT/LVDT power supply, the OE On/Off Registers and the in-channel WDT2. The test uses the +5V Under Voltage Test I/O instructions to trip the voltage monitor into an out-of-tolerance state. The steps below specify an ordering of events with respect to processing.

[IR675:5415;3] All verifications of power supply states shall be made within the tolerances indicated in Table XXXIV.

[IR675:591;415] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

The sequencing of the DCU A and DCU B test sequences will be controlled by means of the Inter-DCU Status Register.

TEST SUMMARY:

The sequence of steps needed to turn on (off) a power supply and to verify that it is turned on (off) are:

- (a) Issue the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.
- (b) Delay 100 +/-10 usec to allow the bits to flip, then verify that the appropriate OE Power Safety Switches are On (Off).
- (c) Turn on (off) the OE A and OE B 2khz RVDT/LVDT power supplies and vary the source of the excitation.
- (d) Energize the Fuel System Purge Solenoids to the Pull-In level, energize the CCV fail-safe servoswitches to provide a load to power supplies.
- (e) Delay 110 +/-10 msec to allow the solenoid and servoswitch power supplies to stabilize.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power Up  
Reset Test (Continued)

- (f) Check that the power supplies are turned on (off) by verifying that the dual port memory inputs are within the ranges established for an "On" ("Off") condition of the power supplies.

This test demonstrates that:

- (g) When the +5V Under Voltage Test I/O instruction is issued by DCU B, WDT2 in CIE B will time-out and the OE B Power Safety Switch will trip causing the OE B power supplies to drop out.
- (h) When the +5V Under Voltage Test I/O instruction is issued by DCU A, WDT2 in CIE A will time-out and the OE A Power Safety Switch will trip causing the OE A power supplies to drop out.

The test sequence is as follows:

- | DCU A  | DCU B  |
|--|--|
| 1. [IR675:591;418] WDT1 and WDT2 shall be continually reset.   | 1. [IR675:591;419] WDT1 and WDT2 shall be continually reset.   |
|  | 2. [IR675:591;420] This DCU B test sequence shall continue upon completion of DCU A test sequence step 10. |
| 2. [IR675:591;421] "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions shall be issued. |  |
| 3. [IR675:591;422] A 100 +/-10 usec delay shall be allowed.  |  |
| 4. [IR675:591;423] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.                             |  |

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power Up Reset Test (Continued)

5. [IR675:591;424] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel B.

6. [IR675:5141;7] Both Fuel System Purge solenoids shall be energized to the Pull-In level. The expected energized state will be verified after the appropriate delay time as required by the Engine-Controller On/Off Devices monitoring of 3.2.3:2.3.5(j).

[IR675:5141;8] Both Fuel System Purge solenoids shall be commanded to the Hold level. Because the solenoids were energized when commanded to the Pull-In level, reverification of the energized state is not necessary for the Hold level.

7. [IR675:591;426] Both CCV fail-safe servoswitches shall be energized.

8. [IR675:5150;5] A 110 +/-10 msec delay shall be allowed following issuance of the "Turn On OE A Power Control Switch" and "Turn On OE B Power Control Switch" I/O instructions.

9. [IR675:591;428] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B, and FRVA/FRVB power supply outputs shall be verified to be On.

10. [IR675:591;429] The SL1/SL2 power supply outputs shall be verified to be at the Hold level.



3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power Up  
Reset Test (Continued)

11. [IR675:4102;19] This DCU A test sequence shall continue upon completion of DCU B test sequence step 8.
  3. [IR675:1386;111] The resetting of WDT2 shall be discontinued.
  4. [IR675:591;433] A "Set +5V Under Voltage Test" I/O instruction shall be issued.
  5. [IR675:591;434] A 100 +/-10 usec delay shall be allowed.
  6. [IR675:591;435] OE A Power Safety Switch shall be verified to be On, and OE B Power Safety Switch shall be verified to be Off.
  7. [IR675:591;436] WDT2 shall be verified to have timed-out.
  8. [IR675:1386;112] A 110 +/-10 msec delay shall be allowed after issuance of "Set +5V Under Voltage Test" I/O instruction.
  9. [IR675:4102;20] This DCU B test sequence shall continue upon completion of DCU A test sequence step 13.
12. [IR675:4102;21] OE1B, OE2B, OE7B, SL2, and FRVA/FRVB power supply outputs shall be verified to be Off.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power Up  
Reset Test (Continued)

13. [IR675:4102;22] All devices controlled by the OE B On/Off Registers shall be verified to be deactivated.
14. [IR675:4102;23] This DCU A test sequence shall continue upon completion of DCU B test sequence Step 11.
  10. [IR675:591;439] A "Reset +5V Under Voltage Test" I/O instruction shall be issued.
  11. [IR675:1386;114] WDT2 shall be continually reset.
  12. [IR675:4102;24] This DCU B test sequence shall continue upon completion of DCU A test sequence step 30.
15. [IR675:591;441] A "Turn On OE B Power Control Switch" I/O instruction shall be issued.
16. [IR675:591;442] A 100 +/-10 usec delay shall be allowed.
17. [IR675:591;443] OE A Power Safety Switch and OE B Power Safety Switch shall be verified to be On.
18. [IR675:591;444] OE A and OE B 2khz RVDT/LVDT power supplies shall be turned on using excitation source from Channel A.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power  
Up Reset Test (Continued)

19. [IR675:5141;9] Both Fuel System Purge solenoids shall be energized to the Pull-In level. The expected energized state will be verified after the appropriate delay time as required by the Engine-Controller On/Off Devices monitoring of 3.2.3:2.3.5(j).

[IR675:5141;10] Both Fuel System Purge solenoids shall be commanded to the Hold level. Because the solenoids were energized when commanded to the Pull-In level, reverification of the energized state is not necessary for the Hold level.

20. [IR675:591;446] Both CCV fail-safe servoswitches shall be energized.
21. [IR675:5150;6] A 110 +/-10 msec delay shall be allowed following issuance of the "Turn On OE B Power Control Switch" I/O instruction.
22. [IR675:591;448] The OE1A/OE1B, OE2A/OE2B, OE7A/OE7B and FRVA/FRVB power supply outputs shall be verified to be On.
23. [IR675:591;449] The SL1/SL2 power supply outputs shall be verified to be at the Hold level.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power  
Up Reset Test (Continued)

24. [IR675:1386;115] The resetting of WDT2 shall be discontinued.
  25. [IR675:591;452] A "Set +5V Under Voltage Test" I/O instruction shall be issued.
  26. [IR675:591;453] A 100 +/-10 usec delay shall be allowed.
  27. [IR675:591;454] OE A Power Safety Switch shall be verified to be Off.
  28. [IR675:591;455] OE B Power Safety Switch shall be verified to be On.
  29. [IR675:591;456] WDT2 shall be verified to be timed-out.
  30. [IR675:5150;7] A 110 +/-10 msec delay shall be allowed following issuance of the "Set +5V Under Voltage Test" I/O instruction.
  31. [IR675:4102;25] This DCU A test sequence shall continue upon completion of DCU B test sequence step 14.
- 
13. [IR675:4102;26] OE1A, OE2A, OE7A, SL1, and FRVA/FRVB power supply outputs shall be verified to be Off.

3.2.3:2.3.5:21 OE Power Safety Switch Voltage Monitor/Power  
Up Reset Test (Continued)

14. [IR675:4102;27] All devices controlled by the OE A On/Off Registers shall be verified to be deactivated.
  
32. [IR675:591;460] A "Reset +5V Under Voltage Test" I/O instruction shall be issued.

3.2.3:2.3.5:22 PSE Power Off Indicator Test

The PSE Power Off Indicator Test verifies that the POI latch is operational.

[IR675:1386;116] This test shall be performed by both DCU A and DCU B.

[IR675:1386;117] Any result other than that which is specified in the test sequence steps below shall constitute failure of this test.

(a) The test sequence is as follows:

- (1) [IR675:591;461] The status of POI shall be determined per POI Set status (see Table XXXVII).
- (2) [IR675:4381;12] POI shall be commanded (see Table XXXVIII) to the state opposite to that found in Step 1. [IR675:4772;1] A delay of at least 5.5 usec shall be allowed.
- (3) [IR675:591;463] The status of POI shall again be determined and verified that POI has achieved the commanded state.
- (4) [IR675:4381;13] POI shall be commanded to resume the state found in Step 1. [IR675:4772;2] A delay of at least 5.5 usec shall be allowed.
- (5) [IR675:591;465] The status of POI shall again be determined and verified that POI has achieved the commanded state.

3.2.3:2.3.5:23 Cross-Channel Power Test

This test is now performed within the PSE Output Voltage Maintenance Monitoring Test of 3.2.3:2.2.2 because the cross-channel power supply levels can be verified without the Group 1 (Sensor Checkout) switches being activated. The activation of the Group 1 switches had been a basic requirement of the test, but is no longer necessary.

3.2.3:2.3.5:24 RVDT/LVDT Excitation Power Supply Source Test

The RVDT/LVDT power supply source test verifies that the OE A and OE B RVDT/LVDT power supplies can be driven by either the Channel A 2khz source or the Channel B 2khz source.

[IR675:1430;8] This test shall be performed by DCU A while operating as the in-control DCU. WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running. [IR675:4597;29] The OE Power Safety Switches shall be turned on by issuing the Turn On OE A/B Power Control Switch I/O instructions.

(a) The test sequence is as follows:

- (1) [IR675:1386;120] The OE On/Off Registers 2A and 2B shall be commanded to the first state (defined below) upon initial entry to this test, or to the next state as specified by ensuing steps of this test.

<u>OE 2A</u> <u>Bit 8</u>	<u>OE 2B</u> <u>Bit 8</u>	<u>FRVA</u>	<u>FRVB</u>
OFF (0)	OFF (0)	OFF	OFF
ON (1)	OFF (0)	ON	ON
OFF (0)	ON (1)	ON	ON
ON (1)	ON (1)	OFF	ON

- (2) [IR675:591;475] A delay of 17 +/-10 msec shall be allowed.
- (3) [IR675:591;476] An IE input sequence of FRVA/FRVB shall be requested.
- (4) [IR675:4381;15] When the input sequence is completed, FRVA and FRVB shall be verified to be in the states defined in step 1. Tolerances for On/Off states are defined in Table XXXIV.
- (5) [IR675:591;478] Failure of any parameter to be within the expected tolerance shall constitute test failure.
- (6) [IR675:1386;121] Each succeeding OE On/Off Register RVDT/LVDT test state shall be invoked by repeating steps 1 through 5.

3.2.3:2.3.5:25 Pneumatic Solenoid Test

This test verifies that each pneumatic solenoid can be commanded to both the Pull-In and Hold states, and that appropriate voltages and currents are properly applied and monitored. It also checks that there is no improper interaction between solenoids.

[IR675:1430;9] This test shall be conducted by DCU A only, while operating as the in-control DCU. WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running. [IR675:4597;30] The OE Power Safety Switches shall be turned on by issuing the Turn On OE A/B Power Control Switch I/O instructions.

[IR675:591;482] The test shall be conducted for each channel (coil) of each solenoid, namely, Bleed Valve Solenoid A and B, Fuel System Purge Solenoid A and B, Emergency Shutdown Solenoid A and B, Pogo Precharge Solenoid A and B, Preburner Shutdown Purge Solenoid A and B, and HPOP IMSL Purge Solenoid A and B.

[IR675:591;483] During performance of this test, the elements of 3.2.3:2.3.5(j) that require the state of all Engine/Controller On/Off devices to be verified to be in their expected states shall be suspended and superseded by the steps of this test.

(a) The test will be conducted as follows:

- (1) [IR675:591;484] The solenoid channel (coil) under test shall be energized at the Pull-In level; all other solenoid coils shall be deenergized.
- (2) [IR675:1386;122] After a delay of 6.5 +/-0.5 msec, SL1 and SL2 shall be requested for input. [IR675:3528;4] Upon completion of input, the parameter corresponding to the solenoid coil under test, SL1 or SL2 (SL1 for a Channel A coil, SL2 for a Channel B coil), shall be verified to be within tolerance for the Pull-In level per Table XXXIV. [IR675:591;486] Failure of the parameter to be within tolerance shall constitute failure of the test.



3.2.3:2.3.5:25 Pneumatic Solenoid Test (Continued)

- (3) [IR675:5143;1] After a delay of 30+/-5 msec from commanding the solenoid coil in step 1, the corresponding solenoid monitor indicator (see Table XXXVII) shall be verified to indicate that the corresponding channel of the solenoid is energized, and that indicators for all other solenoid coils indicate deenergized. [IR675:591;488] Failure to verify these states shall constitute test failure.
- (4) [IR675:591;489] The Solenoid Energize Test (see Table XXXIII) shall be commanded on. The coil current threshold is changed from the Hold to the Pull-In level by the Solenoid Energize Test. Once the test is commanded on, the solenoid coil current comparator designates the solenoids as being energized only if the current remains above the Pull-In level. Any subsequent loading of the OE Storage Register will cancel the test.
- (5) [IR675:591;490] After a delay of 525 +/-25 usec from transferring the command in step 4, the solenoid monitor indicator for the solenoid coil under test shall be verified to indicate that the corresponding channel of the solenoid is energized. [IR675:591;491] Failure to observe this shall result in test failure.
- (6) [IR675:5150;8] After a delay of 35 +/-5 msec from completion of step 5, the solenoid channel under test shall be commanded to the Hold level.
- (7) [IR675:1386;123] After a delay of 6.5 +/-0.5 msec, SL1 and SL2 shall be requested for input. [IR675:4381;16] Upon completion of input, the parameter corresponding to the solenoid coil under test, SL1 or SL2 (SL1 for a Channel A coil, SL2 for a Channel B coil), shall be verified to be within tolerance for the Hold level per Table XXXIV. [IR675:591;495] Failure of the parameter to be within tolerance shall constitute failure of the test.

3.2.3:2.3.5:25 Pneumatic Solenoid Test (Continued)

- (8) [IR675:5150;9] After a delay of 35 +/-5 msec from completion of step 6, the corresponding solenoid monitor indicator shall be verified that the solenoid coil is energized. [IR675:591;497] Failure to observe this shall constitute test failure.
- (9) [IR675:591;498] The solenoid coil under test shall be commanded to be deenergized.
- (10) [IR675:5150;10] After a delay of 35 +/-5 msec from commanding the solenoid in step 9, the corresponding solenoid monitor indicator shall be verified to indicate that the solenoid coil is deenergized. [IR675:591;500] Failure to verify this state shall constitute test failure.

3.2.3:2.3.5:26 Servoactuator Error Indication Interrupt Test

This test verifies that each servoactuator error indication is capable of invoking the proper interrupt processing in both DCUs and that each servoactuator error indication can be properly enabled and disabled in the CIE. The test is performed by generating each servoactuator error indication and verifying that an SEII is serviced.

[IR675:1430;10] This test shall be performed by both DCU A and DCU B each while operating as the in-control DCU. For the in-control DCU, WDT1 and WDT2 will be continually reset; that is, WDT1 and WDT2 will not time-out while this test is running. [IR675:4597;31] The in-control DCU shall turn on the OE Power Safety Switches by issuing the Turn On OE A/B Power Control Switch I/O instructions. [IR675:4597;32] The source of the 2 khz excitation for both OEs shall be selected from the in-control DCU. [IR675:4597;33] A delay of at least 10 msec shall be allowed.

[IR675:591;502] During the performance of this test, the logic that normally services SEIIs shall be inhibited.

[IR675:591;503] Processing of the SEII shall consist of the steps specified within this test.

- (a) [IR675:591;505] The test shall be performed by the following steps for each servoactuator error indication numbered 1 through 5 and 7 through 11:

3.2.3:2.3.5:26 Servoactuator Error Indication Interrupt Test  
(Continued)

- (1) [IR675:591;506] The targeted servoactuator error indication shall be enabled via CIE Interrupt Mask Register Two and the current interrupt level lowered to allow an SEII.
- (2) [IR675:591;507] A servoactuator error indication shall be generated via the Positive Actuator Monitor Test or Negative Actuator Monitor Test, alternating the test type for each SEII generation (see Table XXXIII).
- (3) [IR675:4381;17] It shall be verified that the subject servoactuator error indication interrupt is serviced within 500 usec of commanding the test. [IR675:591;509] Failure of SEII to occur shall constitute failure of the test.
- (4) [IR675:591;510] The servoactuator error indication pending status (see Table XXXVII) shall be verified to indicate an error indication for the targeted servoactuator and no other servoactuator error indications are pending. [IR675:591;511] Failure to verify this configuration shall result in test failure.
- (5) [IR675:591;512] The corresponding OE Storage Register shall be loaded with any pattern in order to terminate the test condition. [IR675:4381;18] A delay of at least 500 usec shall occur.
- (6) [IR675:591;513] All servoactuator error indication pending bits shall be cleared in the CIE by issuing a Clear SEII I/O instruction. [IR675:4381;19] A delay of at least 5.5 usec shall occur.
- (7) [IR675:591;514] The servoactuator error indication pending status shall be verified to indicate that no errors are pending. [IR675:591;515] Failure to verify this indication shall result in test failure.
- (8) [IR675:591;516] The targeted servoactuator error indication shall be disabled in the CIE.

3.2.3:2.3.5:27 Servoalve Driver Current Test

This test is performed as part of Table XXIV, Actuator Checkout.

3.2.3:2.3.5:28 Failure Data Recorder Test

The purpose of this test is to verify that each bit of the FDR's address and data interface can assume both logical states. It is also verified that the FDR address register functions properly by confirming that it decrements by one for each execution of the Decrement Cross-Channel FDR Address Counter I/O instruction.

[IR675:4597;34] This test shall be performed by both DCU A and DCU B.

(a) FDR test patterns will be generated as follows:

The following four steps toggle bits associated with the priority level of the device requesting an interrupt: IPL0, IPL1, and IPL2.

- (1) [IR675:591;530] TRI shall be enabled and processing shall be delayed until a TRI has occurred.
- (2) [IR675:591;531] TRI shall be disabled in the CIE.
- (3) [IR675:591;532] WDT1 shall be enabled in the CIE (WDT1 was timed-out in the prerequisite conditions of 3.2.3:2.3.5). [IR675:4102;32] A sufficient delay shall be allowed for the WDT1 to occur.
- (4) [IR675:591;533] WDT1 shall be disabled in the CIE.

The following two steps toggle the processor status output bits: FC0, FC1, and FC2.

- (5) [IR675:591;534] The DCU Status Register shall be set to the User State.
- (6) [IR675:591;535] The Trap instruction shall be used to return to the Supervisor State.

The following two steps toggle the Address Bits:

- (7) [IR675:4697;5] Location \$FFFFFFE in memory shall be read.

3.2.3:2.3.5:28 Failure Data Recorder Test (Continued)

- (8) [IR675:591;537] Location \$000000 in memory shall be read.

The following two steps toggle the Data word and will complete the R/W bit toggle.

- (9) [IR675:591;538] \$FFFF shall be written into main memory.
- (10) [IR675:591;539] \$0000 shall be written into main memory.

Ensure the patterns stored in the FDR will not be overwritten prior to verification.

- (11) [IR675:724;3] FDR recording shall be inhibited.

The following 2 steps will be performed by the cross-channel in order to verify the in-channel's FDR:

- (12) [IR675:724;4] The 2048 words of data in the Failure Data Recorder shall be scanned by the cross-channel DCU to verify that each bit of Input Words 29 (except bits 7 and 8), 30, and 31 have toggled at least once. FDR SCP Data and Address Error bits (word 29, bits 7 and 8) will be excluded. [IR675:1386;125] Failure of any specified bit to toggle shall result in test failure.
- (13) [IR675:591;545] It shall be verified that the expected FDR Address (in bits 15-5 of Input Word 32) is reached each time the Decrement Cross-Channel FDR Address Counter I/O instruction is commanded. [IR675:1386;126] Failure to attain an expected address shall result in test failure.

3.2.3:2.3.6 Engine Leak Detection Test Support

The Operational Program provides a support function for Engine Leak Detection Tests that are performed by test/flight facility personnel. This support function includes the capability to actuate selected valves on command, maintain them in the commanded state, set the commanded position and ramp rate for the main propellant valves, verify the sensor integrity without the operational constraints required by Sensor Checkout, and command deactivation of all valves.

3.2.3:2.3.6 Engine Leak Detection Test Support (Continued)

[IR687:4785;1] This function shall be activated by any one of the following commands while in the Checkout Standby mode (see Table V):

- (a) Set Propellant Valve Position
- (b) Set Propellant Valve Ramp Rate
- (c) Open OPOV
- (d) Open FPOV
- (e) Open CCV
- (f) Open MOV
- (g) Open MFV
- (h) Open Bleed Valve Control Valve
- (i) Open Fuel System Purge Control Valve
- (j) Open HPOP IMSL Purge Control Valve
- (k) Open Pogo Precharge Control Valve
- (l) Open Preburner Shutdown Purge Control Valve
- (m) Close Emergency Shutdown Control Valve
- (n) Energize Group 1 Sensor Checkout Switches
- (o) Deenergize Group 1 Sensor Checkout Switches
- (p) Energize Group 2 Propellant Drop Sensor Switches
- (q) Deenergize Group 2 Propellant Drop Sensor Switches

Once the function has been activated, the commands:

- (r) [IR687:2001;2] Shall be accepted in a cumulative manner.
- (s) [IR687:2001;3] Shall be accepted in any combination and sequence.
- (t) [IR687:2001;4] Shall be executed as defined below.

The Set Propellant Valve Position and Set Propellant Valve Ramp Rate commands are used to modify the targeted position and ramp rate to be used when a subsequent Open Propellant Valve command is issued. [IR687:1625;1] The targeted position or ramp rate shall apply to any succeeding Open Propellant Valve commands ((c) through (g) given above), but not affect a given valve until that valve is commanded open.

[IR687:1625;2] A command in the range @400 through @64400 shall set the valve position to a value in the range -2% through 102%. [IR687:1625;3] The command shall be decoded as a linear function of the form:

$$\text{(Valve Position)} = 104 / (26880 - 256) \times \text{(Vehicle Command)} + (-3.0)$$

3.2.3:2.3.6 Engine Leak Detection Test Support (Continued)

[IR687:1625;4] A command in the range @64401 through @77740 shall set the ramp rate. [IR687:1625;5] A command in the range @64401 through @77737 shall be decoded as a linear function of the form:

$$\text{(Ramp Rate in \%/sec)} = (12.5/64) \times \text{(Vehicle Command)} + (-5250.0)$$

[IR687:2001;5] Command code @77740 shall correspond to a ramp rate of 5000%/sec, i.e., 100%/major cycle.

[IR688:5768;1] If an Open OPOV, Open FPOV, Open CCV, Open MOV, or Open MFV is accepted, the EMSD Control Valve solenoid shall be energized and the following sequence shall be performed:

- (u) [IR688:5768;2] If the fail-safe servoswitch on any of the five actuators is deenergized, the following shall be performed:
  - (1) Execute an Actuator Pre-operational Conditioning Cycle, per 3.2.3:2.3.8, on all five valves in parallel.
  - (2) Energize the fail-safe servoswitches on all five actuators.
  - (3) Delay 20 msec.
- (v) [IR689:1625;2] The propellant valve shall then be ramped to the position and at the ramp rate last specified by the Set Propellant Valve Position and Set Propellant Valve Ramp Rate commands.

The default position will be 100% open and the default ramp rate will be 100%/sec, as set by Controller Reset. [IR690] The servoswitches and final valve position commands shall be maintained.

[IR691:1386;1] Upon acceptance of a command to energize a purge system control valve ((h) through (l) given above), the Operational Program shall activate both solenoids of the indicated control valve and maintain them in the activated state.

### 3.2.3:2.3.6 Engine Leak Detection Test Support (Continued)

[IR692:2625;1] Upon acceptance of a command to close the Emergency Shutdown Control Valve, the Operational Program will disable CCV servoactuator error indications (3.2.3:6.1.3), shall energize Channel A and B fail-safe servoswitches, and shall energize both Emergency Shutdown Control Valve solenoids for Engine Leak Detection. Only entry into Checkout Standby can enable the CCV servoactuator error indication.

[IR692:4785;1] Upon acceptance of a command to either energize the Group 1 Sensor Checkout Switches or deenergize the Group 2 Propellant Drop Sensor Switches, Propellant Drop monitoring shall be suspended. [IR692:4785;2] Propellant Drop monitoring shall be reinstated while in Engine Leak Detection mode anytime the Group 1 Sensor Checkout Switches are deenergized and the Group 2 Propellant Drop Sensor Switches are energized. [IR692:4785;3] Upon exit from Engine Leak Detection Support mode, the Group 1 Sensor Checkout Switches shall be deenergized, Group 2 Propellant Drop Sensor Switches energized, and Propellant Drop monitoring resumed.

Engine Leak Detection Test Support will be exited upon acceptance of a Controller Reset (3.2.3:1.1.1), Checkout Standby (3.2.3:1.1.2), or Deactivate All Valves (3.2.3:2.3.7) command, or upon occurrence of any I-response.

### 3.2.3:2.3.7 Deactivate All Valves

The Deactivate All Valves command is used to close all propellant valves hydraulically during component checkout.

[IR704:2763;1] When a Deactivate All Valves command is accepted the following sequence shall be executed:

- (a) Energize all fail-safe servoswitches.
- (b) Deenergize all pneumatic solenoids.
- (c) Command all actuators to their current positions and wait 20 msec.
- (d) Ramp all actuator commands to full closed at 100%/second and wait 1.06 seconds for the ramp to complete.
- (e) Return to Checkout Standby per 3.2.3:1.1.2.

### 3.2.3:2.3.8 Actuator Pre-operational Conditioning Cycle

The Actuator Pre-operational Conditioning Cycle will be performed as a prelude to Engine Leak Detection Support (Open Valve commands), Actuator Checkout, Emergency Shutdown Control Valve portion of Pneumatic Checkout, Hydraulic Conditioning, and FRT-1.



### 3.2.3:2.3.8 Actuator Pre-operational Conditioning Cycle (Continued)

When this sequence is invoked as a prelude to a component checkout test, the Step Number will remain 0 during this sequence.

- (a) [IR704:6152;1] The 300 msec sequence shall be as follows:
- (1) Suspend SEII monitoring and the OE Servoactuator Model/Monitor Self-Test. Energize the fail-operational and both fail-safe servoswitches for the selected servoactuator.
  - (2) Delay 40 msec.
  - (3) Save the initial position of the servoactuator. Command Channel A of the servoactuator to +15%.
  - (4) Delay 60 msec.
  - (5) Verify that the servoactuator position is not more than 1% different from the initial position. If this test fails, post an appropriate FID at the end of the sequence. Command Channel A of the servoactuator to 0%.
  - (6) Delay 40 msec.
  - (7) Deenergize the fail-operational servoswitch.
  - (8) Delay 20 msec.
  - (9) Command Channel B of the servoactuator to +15%.
  - (10) Delay 60 msec.
  - (11) Verify that the servoactuator position is not more than 1% different from the initial position. If this test fails, post an appropriate FID at the end of the sequence. Command Channel B of the servoactuator to 0%.
  - (12) Delay 60 msec.
  - (13) Deenergize both fail-safe servoswitches.
  - (14) Delay 20 msec.
  - (15) Resume SEII monitoring and the OE Servoactuator Model/Monitor Self-Test.

If Channel A of the servoactuator is qualified, the position used will be Channel A; otherwise, it will be Channel B.

3.2.3:2.3.8 Actuator Pre-operational Conditioning Cycle  
(Continued)

The Actuator Pre-operational Conditioning Cycle is diagrammed for information only in Figure 11B.

- (b) [IR704:6152;2] If this sequence results in an I-response while in a Component Checkout mode, the checkout test shall be aborted and Checkout Standby mode shall be entered.
- (c) [IR704:6152;3] When in the FRT-1 configuration, if an I-response occurs which is not a result of the pre-operational sequence, the sequence shall be terminated and the following steps performed:
  - (1) Deenergize the fail-safe servoswitches.
  - (2) Command Channel A and B of the servoactuator to 0%.
  - (3) Delay the resumption of SEII monitoring and the OE Servoactuator Model/Monitor Self-Test for three major cycles.
- (d) [IR704:4838;1] Upon completion or termination of this sequence, the fail-operational servoswitches shall be set to the state dictated by the hardware qualification status.
- (e) [IR704:6152;4] If a servoactuator has previously failed this sequence, the sequence for the failed servoactuator shall be bypassed until a Controller Reset command is issued.

3.2.3:2.3.9 Hydraulic Conditioning

[IR704:4320;4] This sequence shall be initiated upon acceptance of a Hydraulic Conditioning command. The sequence is as follows:

- (a) [IR704:5386;1] The Emergency Shutdown solenoid and all fail-safe servoswitches shall be energized.
- (b) [IR704:5386;2] After a 2.0 second delay to vent pneumatic pressure, the fail-safe servoswitches shall be deenergized.
- (c) [IR704:4320;7] An Actuator Pre-operational Conditioning Cycle shall be performed, per 3.2.3:2.3.8, on all five actuators in parallel.  
[IR704:5768;1] At the completion of the Actuator Pre-operational Conditioning Cycle, the fail-safe servoswitches on all five actuators shall be energized.

3.2.3:2.3.9 Hydraulic Conditioning (Continued)

- (d) [IR704:4320;8] The Hydraulic Conditioning Sequence per Table XXIII shall be performed on each actuator (MFV, MOV, CCV, FPOV, OPOV) in series.
- (e) [IR704:4320;9] Upon completion or termination of this sequence, the Emergency Shutdown solenoid, fail-safe servoswitches, and fail-operational servoswitches shall be deenergized unless overridden by disqualification of hardware components (3.2.1:6).

During each major cycle of the Hydraulic Conditioning sequence:

- (f) [IR704:4320;10] The Hydraulic Pressure shall be monitored to be 2650 psia or greater. [IR704:4526;3] If IE B is temporarily or permanently disqualified, this test shall be bypassed. [IR704:4611;1] If the Hydraulic Pressure is out of limits for three consecutive major cycles, this shall constitute a failure.
- (g) [IR704:4320;11] The position of each actuator that is not being commanded shall be monitored to be less than or equal to 3% open. [IR704:4611;3] A failure shall occur if this condition is not met.
- (h) [IR704:4611;4] If an I-response occurs as a result of a Hydraulic Pressure failure, the sequence shall halt at the end of the step in which the failure was detected. [IR704:4611;5] An appropriate Resume command shall cause resumption of the Hydraulic Conditioning sequence with the step following the one in which the failure was detected.

The Hydraulic Conditioning sequence is diagrammed for information only in Figure 12.

Upon completion of the sequence, the Operational program will return to Checkout Standby.

3.2.3:2.4 Flight Readiness Test (FRT) Configurations

The FRT-1 and FRT-2 Configurations provide the capability to exercise the Operational Program in all the engine phases/modes accessible to the Flight Configuration (Table IV). It also allows verification of the vehicle/engine interface, the operational logic and the controller response to a number of simulated failures.

3.2.3:2.4.1 FRT Operation

When the memory configuration is FRT-1 or FRT-2, Propellant Drop Monitoring will be performed. [IR705:3300;1] Additionally, the FRT configurations shall on command, perform the FRT mode operations whereby appropriate engine sensor inputs are simulated.

3.2.3:2.4.1:1 FRT Mode

[IR706:3300;1] When the Activate FRT Simulation command is executed, the FRT mode shall be activated and the ESW shall be updated accordingly. When the configuration is FRT-1 or FRT-2, any Start Preparation command will be rejected if the FRT mode is not active.

3.2.3:2.4.1:1.1 FRT-1

[IR707:3300;1] The Operational Program in the FRT-1 configuration with the FRT mode active shall provide the same performance and responses as the Flight Configuration with the following exceptions.

- (a) VDT ID word 1 and ID word 2 will indicate the configuration is FRT-1 and the ESW will indicate the FRT Status is FRT mode.
- (b) [IR709:2001;1] Simulated engine sensor inputs, as defined in 3.2.3:2.4.2, shall be computed and used.
- (c) However, Propellant Drop Monitoring will be performed per 3.2.3:2.1 utilizing actual sensor input data, ensuring there are no propellants in the engine. A Terminate Checkout Sequence, 3.2.4:4, will be executed if the conditions are not met.
- (d) The OPOV command limit for Thrust Limiting will be set to 100%.
- (e) [IR715:2307;1] The Pogo GOX Flow Check (3.2.3:6.5) shall be bypassed.
- (f) [IR715:2042;1] The Pulse Rate Converter Self-Test for the HPFP Shaft Speed (3.2.3:3.3.2:2) and the Fuel Flowrate (3.2.3:3.3.2:3) shall be bypassed.

In providing this operation, the engine and its support systems are assumed to be operational. This includes the Hydraulic Pressure System, the Pneumatic Control and Purge System and the Electric Power System.

[IR715:4320;1] Upon acceptance of an Enter FRT-1 command, an Actuator Pre-operational Conditioning Cycle, per 3.2.3:2.3.8, shall be performed on all five actuators in parallel.

3.2.3:2.4.1:1.1 FRT-1 (Continued)

[IR716:1413;1] When an Inhibit Igniters in FRT-1 command is accepted, igniters shall not be energized. [IR716:3300;1] This condition shall remain in effect until deactivation of the FRT Mode.

[IR716:3479;1] Upon acceptance of a Shutdown Pneumatically in FRT-1 command, Pneumatic Shutdown shall be performed. The existing FRT-1 configuration will be retained.

3.2.3:2.4.1:1.2 FRT-2

[IR717:3300;1] FRT-2 configuration shall provide the same basic capabilities as FRT-1 configuration except that during the FRT mode additional engine control functions shall be simulated to minimize the cycling of propellant valves and Engine/Controller on/off devices during simulated engine operations.

The following details the additional requirements for FRT-2.

- (a) VDT ID word 1 and ID word 2 will indicate the configuration is FRT-2 and the ESW will indicate the FRT Status is FRT Mode.
- (b) [IR719:2818;1] No fail-safe, fail-operational servoswitches; no pneumatic solenoid valves, and no igniters shall be energized (turned on).
- (c) [IR720] Actuators shall not be commanded.
- (d) Additional parameters will be simulated per 3.2.3:2.4.2.
- (e) All servoactuator error indications will be disabled in the CIE, thus ensuring that SEII monitoring will not be performed (3.2.3:6.1.3).
- (f) [IR728] The Simulate Channel A Failure and Simulate Channel B Failure commands shall not be accepted.
- (g) [IR729:2218;1] Backdoor Purge Initiation Monitoring (3.2.3:5.5) shall be suspended.
- (h) [IR729:3070;1] The Actuator Settling Check (3.2.3:6.1.7) shall be bypassed.

3.2.3:2.4.1:2 Normal Deactivation of FRT Mode

The FRT mode is normally deactivated by using the Deactivate FRT Simulation command. This command is normally transmitted when no failure simulation is in effect and when the engine phase/mode is Checkout Standby or Post Shutdown Standby.

[IR730:3300;1] When a Deactivate FRT Simulation command is executed, the FRT mode shall be deactivated, the ESW shall be updated accordingly and

- (a) [IR730:2049;2] If Pneumatic Shutdown is in effect, it shall be completed leading to Post Shutdown Standby.
- (b) [IR730:2049;3] Else, if not in Pneumatic Shutdown, Post Shutdown Standby shall be entered.

A Deactivate FRT Simulation command received when a DCU A/OE A or DCU B/OE B failure simulation is in effect or during a phase/mode other than the Standby modes stated above, may result in extraneous failure indications.

3.2.3:2.4.1:3 Off-Nominal Deactivation of FRT Mode

The FRT mode (sensor simulation) will be deactivated for the following off-nominal conditions, i.e., other than Deactivate FRT Simulation command:

- (a) If Propellant Drop Monitoring (3.2.3:2.1) constraints are violated, a Terminate Checkout Sequence response will be performed per 3.2.4:4.
- (b) After acceptance of the Controller Reset or Checkout Standby command, Checkout Standby will be entered as defined in 3.2.3:1.1.1 and 3.2.3:1.1.2, respectively.

In both cases above, extraneous failure indications may result depending on the conditions existing at the time of FRT termination.

3.2.3:2.4.2 Engine Simulation

[IR733:3300;1] When the FRT mode is active, engine sensor measurements shall be synthesized (computed) using an engine simulation model. [IR734] Different models shall be used depending on the simulated engine phase/mode. [IR735:6164;1] The simulated parameters and their correlation functions shall be as defined in Table XXII, per the following sections:

- (a) Part A, for Purge Sequence 4 and Engine Ready modes during either FRT.
- (b) Part B for Start, Mainstage and Shutdown phases when the simulated MCC Pc is below 40% RPL during either FRT.
- (c) Part C for Start, Mainstage and Shutdown phases when the simulated MCC Pc is no less than 40% RPL during either FRT.
- (d) Part D for additional simulations required during FRT-1.
- (e) Part E for additional simulations required during FRT-2.

[IR736] For other phases/modes, the actual sensor channel inputs shall be used.

[IR737] Simulated sensor data shall override actual sensor inputs, as soon as the indicated phases/modes are entered. Simulated data will be inserted so as to exercise, to the extent possible, all applicable software routines in the same manner as during actual flight operations. It is acceptable that the simulated sensor data be inserted as scaled values, and the Sensor Input Data Scaling function (3.2.3:4.1) be bypassed if significant software simplification results.

The process of converting from a number representing the physical units of the measured parameter to an IE DPM value

### 3.2.3:2.4.2 Engine Simulation (Continued)

is called inverse scaling. [IR739:2452;1] Where simulated sensor measurements are to be inserted as unscaled inputs, the FRT simulation model shall use a single inverse scaling function for all channels of a sensor. [IR739:2452;2] All inverse scaling functions shall use nominal scaling coefficients. [IR740] However, the RVDT outputs of OPOV and FPOV shall be scaled per their individual calibration coefficients to compute percent opening of full-scale.

[IR741:3300;1] When the configuration is FRT, data processing and monitoring to verify that there are no propellants present (Propellant Drop Monitoring, 3.2.3:2.1) shall be performed on actual sensor inputs rather than simulated parameter values.

### 3.2.3:2.4.3 Failure Simulations

[IR742:3300;1] The FRT configurations shall have the capability to simulate failures of the engine or controller on command, as defined below.

The purpose is to exercise the failure response capability and logic in these selected cases. The Simulate Channel A/B Failure commands may be used during FRT-1 only, not during FRT-2. However, the Simulate Out-Of-Limits command will be accepted during either FRT.

#### 3.2.3:2.4.3:1 DCU A/OE A and DCU B/OE B Failure Simulations

[IR744] Acceptance of a Simulate Channel A or Simulate Channel B Failure command during FRT-1 shall cause simulation of failure of the selected DCU and OE. [IR745:1843;1] The response for a simulated disqualification of a DCU shall be per 3.2.1:6.1, 3.2.1:6.5, and 3.2.4.

[IR745:1843;2] The response for a simulated disqualification of an OE shall be per 3.2.3:2.4.3:1.1. [IR747] To ensure proper timing coordination with the cross-channel DCU, the in-channel failure response shall be executed 25 to 45 msec after command acceptance.

[IR748:1843;1] The cross-channel DCU, if not previously failed in actuality or by simulation, shall anticipate the simulated DCU failure within 45 msec upon acceptance of the command.

[IR748:1843;2] If an RCFI is received within 45 msec after command acceptance, the cross-channel DCU shall simulate a disqualification of the selected DCU and OE channels.

[IR751:1843;1] If an RCFI is received subsequent to 45 msec, it shall be interpreted as an actual DCU failure, and the cross-channel DCU shall not simulate an OE failure.



3.2.3:2.4.3:1 DCU A/OE A and DCU B/OE B Failure Simulations (Continued)

Hardware detection of an in-channel Reset Channel command with Halt Exit enabled will cause the DCU to enter PROM. Acceptance of a subsequent Exit PROM command will result in pneumatic shutdown culminating in Post-Shutdown Standby (3.2.1:2.2.1) Flight configuration. The cross-channel DCU will then reset all indications of OE and servoactuator failures (3.2.1:2.2.1) if it has been a simulated failure (not an actual one).

[IR755] The Simulate Channel A/B Failure commands shall be rejected when received during FRT-2.

[IR756:3300;1] With the operation defined above, FRT failure simulation shall not result in any extraneous failure indication if FRT mode is ended with each DCU/OE in the same operational (failure) status as when FRT mode was started.

3.2.3:2.4.3:1.1 Simulated Disqualification of an OE Channel

This response is similar to an actual OE Channel disqualification except propellant drop checks (3.2.3:2.1) and most OE self-tests will be maintained. A record will be kept which distinguishes a simulated OE failure and simulated servoactuator failures from actual failures.

[IR757:1364;1] A simulated failure of either OE Channel A or B shall result in the following responses for the respective OE channel:

- (a) [IR757:1364;2] All solenoids shall be deenergized.
- (b) [IR757:1364;3] All fail-safe servoswitches shall be deenergized.
- (c) [IR757:1364;4] All igniters shall be deenergized.
- (d) [IR757:1364;5] The Group 1 (Sensor Checkout) switches shall be deenergized. The Group 2 (Propellant Drop Sensor) switches will remain energized.
- (e) [IR757:1364;6] The PRC Overflow Test shall be deactivated.
- (f) Halt Exit will remain disabled.

3.2.3:2.4.3:1.1 Simulated Disqualification of an OE Channel  
(Continued)

- (g) [IR757:1386;1] If the source of RVDT/LVDT excitation is to be switched to CIE B during the ensuing simulated disqualification of the servoactuators, the OE A Power Control Switch shall be commanded off after 20 +/- 10 msec to allow the fail-operational switches to take effect. [IR757:3528;1] Else the source of excitation will be retained, and the OE Power Control Switch shall be commanded off immediately subsequent to the suspension of SEII monitoring in 3.2.3:6.1.3.
- (h) [IR757:1386;3] There shall be no other commands transmitted to the OE channel with the simulated failure except for:
  - (1) Commanding the OE Power Control Switch off each major cycle.
  - (2) Updating the OE Power Control Switch and the OE On/Off Registers in Major Cycle Restart, 3.2.1:2.3(d) (1).
- (i) [IR757:3528;2] As the final response, simulated disqualification of the servoactuators on the respective channel shall be accomplished by performing the requirements for actual disqualification.

3.2.3:2.4.3:2 Preburner Over-Temperature Simulation

[IR758:1843;1] Acceptance of a Simulate Out-Of-Limits command, during either FRT, shall cause simulation of over-temperature of the HPOT Discharge Temperature by setting the parameter to a value representing 2282 degrees R in the engine simulation models of Table XXII, Part B and Part C. As the simulated high reading is inserted for use by the Flight Configuration routines, Shutdown Limit Monitoring Failure Response will result, initiating Engine Shutdown as defined in 3.2.3:5.3.1.

[IR759:3300;1] The substitution of a high-temperature value for HPOT Discharge Temperature shall be discontinued (negated) when the FRT mode is deactivated.

### 3.2.3:3 Controller Continual Self-Tests

Tests described in the following subordinate paragraphs are those that are performed in conjunction with major cycle processing both during pre-flight program execution and during flight. They are designed to provide a reasonable level of controller component testing while not interfering with the timing requirements of engine control functions. The execution of these tests, together with the mechanisms of the self-checking pair processors, are the primary tools for managing the controller redundancy during flight.

Requirements that are generally applicable to all the following subordinate self-tests are as follows:

- (a) [IR759:591;1] These tests shall be performed only during major cycle processing. Provisions have been made to separately define the requirements for self-tests during periods when the program is executing in a non-major cycle manner. No tests will be performed involving access to elements of a channel being monitored for power recovery, per 3.2.1:9.3.1(e).
- (b) All failures of these tests will be reported per 3.2.4.
- (c) [IR759:591;3] Whenever a verification is required within a range expressed as  $X \pm Y$  time units, the test shall perform the verification at any time within the range in order to check if the step has passed or failed.
- (d) [IR759:591;4] Whenever a self-test refers to failures for differing parameters on an IE channel, those parameters shall be only those as specified within that self-test.
- (e) Whenever a self-test refers to a parameter being within some percentage value, this implies a plus or minus percentage.
- (f) [IR759:591;5] Minimum and maximum limits for a parameter shall be inclusive values.
- (g) Some self-tests define minimum delay periods during which the test is suspended. [IR759:591;6] If such a self-test is performed on a major cycle basis, then the test shall be reactivated no later than the major cycle following the completion of the delay. Design may reactivate the test earlier as long as the minimum delay time is not violated.

3.2.3:3 Controller Continual Self-Tests (Continued)

- (h) Whenever a self-test refers to a pair of parameters with a slash between them, for example RC03/RC02, this indicates a Channel A parameter followed by a Channel B parameter. Single parameters will be identified as either (Ch A) or (Ch B).
- (i) In some self-tests when an error occurs upon the first attempt to run the test, an immediate retry or immediate reread is required for a second attempt. A failure is detected if the error persists upon the second attempt. If the second attempt cannot be accomplished within the same major cycle in which the error was first noted (for instance a power transient intervenes), the second attempt is abandoned. Such attempts differ from strikes in that the attempts are to be accomplished within the same major cycle, whereas strikes occur over several major cycles. [IR759:3528;1] Because strike counts tally errors that occur over several major cycles, strike counts shall not be applicable to those self-tests requiring an immediate retry or immediate reread.
- (j) [IR759:3528;2] Within a major cycle only the first detected failure within a self-test shall have its failure response invoked by the self-test, unless specified otherwise.

The continual self-tests have been categorized into one of three groupings depending on the primary nature of the test. The three groupings are (1) Event Driven Self-Tests, (2) Periodic Self-Tests, and (3) IE DPM Data Qualification/Verification Self-Tests.

3.2.3:3.1 Event Driven Self-Tests

These self-tests are performed primarily as part of the execution of an independently required event. They are designed to qualify or verify proper operation of the electronic hardware associated with the required event.

3.2.3:3.1.1 VEEI Command MUX Self-Test

[IR759:591;7] The VEEI Command MUX Self-Test shall be performed by reading the test patterns of the two Command MUX Test Words (see Table XXXVII) to verify that each of the 16 command MUX data bits can be toggled. [IR759:591;8] This self-test shall be performed by both DCU A and DCU B in conjunction with each instance of that DCU reading the VEEI Command Registers per 3.2.2:1.

3.2.3:3.1.1 VEEI Command MUX Self-Test (Continued)

A failure within this self-test occurs when either test word does not match the expected value. [IR759:4381;1] This self-test shall be considered to have failed after two successive failures (immediate reread).

[IR759:591;10] The response to failure of this self-test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.1.2 CIE Inter-DCU Status Register Self-Test

The Inter-DCU Status Registers provide communication links between DCUs. The primary function of this communication is transmission of phase/mode, ignition confirmation, and disqualification status data from the in-control DCU to the standby DCU.

The purpose of the CIE Inter-DCU Status Register Self-Test is to effect this communication while maintaining the integrity of the communication link. This is accomplished by the protocol below.

- (a) Status data is written by DCU A to IDSR A.
- (b) DCU B acknowledges receipt of the status word by writing ("reflecting") the status word to IDSR B.
- (c) DCU A confirms that the data reflected by DCU B is correct by writing the complement of the status word to IDSR A.
- (d) DCU B acknowledges receipt of the confirmation word by reflecting the confirmation word to IDSR B. At this point, the confirmed status data is validated for use.

This self test is comprised of 4 major components; input of cross-channel IDSR data, determination of the next pattern to be transmitted, write/read check of data to the in-channel IDSR, and reaction to and reflection of the pattern received.

[IR759:1789;1] Unless suspended, this test shall be performed once each minor cycle by each DCU. [IR759:3494;1] This test shall be suspended when normal major cycle processing is suspended by either DCU. This will occur if either DCU is not operational, or during a power transient, Controller Checkout, portions of Actuator Checkout, Igniter Checkout, or conditions resulting in a Major Cycle Restart. [IR759:3550;1] Upon recovery from suspension, or upon acceptance of a Controller Reset command, IDSR conditions shall be established to effect an output by DCU A of an Engine Data Word (EDW) as defined in Table XLII.

3.2.3:3.1.2 CIE Inter-DCU Status Register Self-Test  
(Continued)

[IR759:1789;5] During each minor cycle, each DCU shall perform two consecutive reads of the cross-channel IDSR.

[IR759:1789;6] If the values are equal and differ from the previous valid update of the cross-channel IDSR, a valid update shall be established.

For DCU A,

[IR759:1789;7] If a valid update of the IDSR B value is established and agrees with the current value of IDSR A, then the value in IDSR B is a valid reflection, and a new pattern shall be determined as described in 3.2.3:3.1.2:2 Determine Pattern, and written to IDSR A.

Otherwise, no valid reflection from DCU B has been established, and the current value of IDSR A will be retained.

For DCU B,

[IR759:1789;8] If a valid update of IDSR A is established, then the value in IDSR A is a valid new pattern, and a value shall be determined as described in 3.2.3:3.1.2:3 Reflect Pattern, and written to IDSR B.

Otherwise, no valid new pattern from IDSR A has been established, and the current value of IDSR B will be retained. [IR759:4402;1] If a valid update has not been established within 7 consecutive minor cycles, then DCU B shall perform self-disqualification.

[IR759:1789;10] Subsequent to Determine Pattern for DCU A, or Reflect Pattern for DCU B, the IDSR Write/Read Check (3.2.3:3.1.2:1) shall be performed.

3.2.3:3.1.2:1 IDSR Write/Read Check

[IR759:1789;11] Under the conditions prescribed in 3.2.3:3.1.2, during each minor cycle each DCU shall perform an IDSR Write/Read Check by reading the in-channel IDSR and comparing that value to the value last loaded (written) into the in-channel IDSR. [IR759:1789;12] If the value read and the value loaded do not agree, the DCU shall immediately reread the IDSR. [IR759:1789;13] If the reread also fails, the DCU shall disqualify itself. Self disqualification is performed because failure of the write/read check may be caused by a common data bus error undetectable by other means.

3.2.3:3.1.2:2 Determine Pattern (DCU A: React to IDSR B)

[IR759:1789;14] If the current IDSR A (value transmitted by DCU A in the previous minor cycle) is not an Engine Data Word (EDW), then an EDW formatted according to Table XLII shall be loaded into IDSR A.

[IR759:1789;15] Otherwise, the current IDSR A is an EDW, and the ones complement of the current EDW shall be loaded into IDSR A.

3.2.3:3.1.2:3 Reflect Pattern (DCU B: React to IDSR A)

[IR759:1789;16] When invoked under these conditions prescribed in 3.2.3:3.1.2, the value read from IDSR A, shall be loaded into IDSR B for reflection back to DCU A.

[IR759:1789;17] If the IDSR A value is an EDW, then the EDW shall be saved as the tentative new EDW. [IR759:1789;18] Otherwise, the IDSR A value is a confirmation word, and if the current and previous values are complementary, the previously received tentative EDW shall be qualified for use and designated the validated Engine Data Word.

3.2.3:3.1.3 VRC Dual Port Memory Self-Test

[IR759:591;41] The VRC DPM Self-Test shall verify that the first 32 words of the VRC Dual Port Memory have been updated with valid data before each VRC transmission. [IR759:591;42] This test shall be performed prior to each VRC transmission by the DCU in control of VRC transmission. The DCU accomplishes this by accessing the addresses in the VRC DPM that are dedicated to these words (see Table XXXV), thus reading back the contents of each word. Each read allows the SCP data bus comparators to verify the data match between the two VRC DPMs.

Failure of this test is detected by the generation of the SCPI, which will result in the disqualification of the DCU/CIE that had the error.

3.2.3:3.1.4 Real Time Clock/IE Timing Self-Test

The Real Time Clock/IE Timing Self-Test verifies the RTC/IE timing and the integrity of the independent clocks that drive them. The test verifies that the expected number of words have been input during a specified period of time within the IE input sequence process. This test will be performed by comparing elapsed time as measured by the Real Time Clock with the time it took to input the number of words as derived from the IE Address Counter. [IR759:591;43] This test shall be performed by the in-control DCU, in conjunction with each request for all sensor inputs via an IE input sequence per 3.2.1:2.1.

3.2.3:3.1.4 Real Time Clock/IE Timing Self-Test (Continued)

The test sequence follows:

- (a) [IR759:3105;1] The current interrupt level shall be set to 4.
- (b) [IR759:3105;2] Immediately after the execution of the Initiate IE Operation I/O Instruction (which initiates the IE conversion of sensor inputs per 3.2.1:2.1), the following shall be performed:
  - (1) [IR759:591;46] The value of the RTC Output (see Table XXXVII) shall be read and retained.
  - (2) [IR759:628;5] The current interrupt level shall be reinstated to the condition that prevailed prior to (a).
- (c) [IR759:591;47] After the next TRI (which defines the start of minor cycle #1) and prior to completion of the IE input sequence, the following shall be performed:
  - (1) [IR759:628;6] The current interrupt level shall be set to 4.
  - (2) [IR759:3280;1] Four successive reads of the IE Address Counter shall be performed to retain four successive values.
  - (3) [IR759:591;49] The value of the RTC Output shall be read and retained.
  - (4) [IR759:628;7] The current interrupt level shall be reinstated to the condition that prevailed prior to (1).
  - (5) [IR759:591;50] The elapsed time, which is the difference between the retained RTC Output values adjusted for RTC rollover, shall be calculated.
  - (6) [IR759:3280;2] The input time based on the 50 usec required for the conversion and input of each sensor pair shall be calculated. The input time is 50 usec multiplied by the retained IE Address Counter value that has remained invariant for at least two successive reads.



3.2.3:3.1.4 Real Time Clock/IE Timing Self-Test (Continued)

- (7) [IR759:3280;3] If the IE Address Counter values have not remained invariant for at least two successive reads, the DCU/CIE that detected the error shall be disqualified.

[IR759:3280;4] The test shall be considered passed if the elapsed time equals the input time within a tolerance of -12 to +72 usec.

[IR759:591;53] The test shall be considered failed if the difference between the elapsed time and the input time is not within the tolerance.

[IR759:591;54] The response to a single failure of this test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.1.5 Interrupt Decoder Self-Test

The Interrupt Decoder Self-Test verifies that an interrupt is pending and, in most cases, enabled by the CIE when the DCU responds to the interrupt. [IR759:591;55] This test shall be performed by both DCU A and DCU B.

The test is performed within the processing that services those interrupts identified as vector numbers 64 through 73 inclusive (see Table XL). [IR759:591;56] This processing shall verify that the corresponding interrupt is pending (see Table XXXVII). [IR759:591;57] If the interrupt is not pending the test shall be considered to have failed.

Interrupts, other than PFI and PRI (vectors 64 and 65), can be enabled by means of the CIE interrupt mask registers (see Table XXXIX). In order for the processing to verify that the corresponding interrupt is enabled, the current status of the corresponding CIE interrupt mask register is retained in RAM. Each time a CIE interrupt mask register is loaded, its corresponding software status is updated. [IR759:591;59] When an interrupt is serviced, the software status of the corresponding CIE interrupt mask register should indicate that the interrupt is enabled, and if it is not, the test shall be considered to have failed.

[IR759:591;60] The response to a single failure of this test shall be to disqualify the DCU/CIE that detected the error.

[IR759:3020;1] If PFI is not pending at the time it was serviced, the self-disqualification of the DCU/CIE shall be performed during the In-Channel Power Recovery Response of 3.2.1:1.6.

3.2.3:3.1.6 IE Sequencer Self-Test

The IE Sequencer Self-Test verifies the proper initialization and completion of the IE address/range counters and the corresponding channel and completion indicators for each IE input sequence.

[IR759:2168;1] This self-test shall be performed each major cycle, in conjunction with the IE input sequence of 3.2.1:2.1.  
 [IR759:1386;1] For an IE input sequence of some, but not all of the parameters of the entire IE DPM, only subparagraph (a) of the ensuing test sequence shall be performed.  
 [IR759:591;62] This self-test shall be performed only by the in-control DCU.

The test sequence follows:

- (a) [IR759:591;63] After the in-channel IE Address Counter and IE Range Counter have been loaded with initial values, the following shall be performed:
  - (1) [IR759:591;64] The contents of the in-channel counters shall be read (see Table XXXVII) and compared with the loaded data to verify that they are equal.
  - (2) [IR759:591;65] The in-channel IE Channel Indicator shall be verified to indicate Channel A.
  - (3) A failure within this test occurs when the value read for either IE counter does not equal the loaded value, or when the IE Channel Indicator does not indicate Channel A.
  - (4) [IR759:591;66] This self-test shall be considered to have failed after two successive failures (immediate retry). [IR759:591;67] Failure of the retry shall result in disqualification of the DCU/CIE that detected the error.
- (b) [IR759:591;68] After a 6.5 msec minimum delay and before the initiation of the next IE input sequence, the following shall be performed:
  - (1) [IR759:591;69] The in-channel IE Conversion Complete shall be verified to indicate conversion complete.
  - (2) [IR759:591;70] The in-channel IE Channel Indicator shall be verified to indicate Channel B.

3.2.3:3.1.6 IE Sequencer Self-Test (Continued)

- (3) [IR759:591;71] The in-channel IE Range Counter shall be verified to contain zero.
- (4) [IR759:591;72] The in-channel IE Address Counter shall be verified to contain a value equal to the sum of the initial IE Address Counter contents and the initial IE Range Counter contents.
- (5) A failure within this test occurs when any one of the preceding checks fail to pass verification.
- (6) [IR759:591;73] A single failure shall cause disqualification of all IE DPM data during the major cycle in which the error was detected. [IR759:591;74] This self-test shall be considered to have failed after two successive failures. [IR759:591;75] The response to failure of this self-test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.1.7 OE Storage Registers Self-Test

The OE Storage Registers Self-Test verifies the proper loading of OE A Storage Register and OE B Storage Register before the contents of the storage registers are transferred to the selected output devices, unless specifically exempted. [IR759:591;76] This self-test shall be performed only by the in-control DCU.

[IR759:591;77] After the OE A Storage Register and OE B Storage Register have been loaded with initial values (see Table XXXVIII), the contents of the registers shall be read (see Table XXXVII) and compared with the loaded data to verify that they are equal.

A failure within this test occurs when the value read for either storage register does not equal the loaded value.

[IR759:591;78] This self-test shall be considered to have failed after two successive failures (immediate retry). [IR759:4934;1] The failure response for this self-test shall be to immediately discontinue transferring data from this storage register and to disqualify the affected OE.

3.2.3:3.1.8 Watchdog Timer Status Self-Test

[IR759:591;80] The Watchdog Timer Status Self-Test shall be performed as part of TRI processing that routinely resets the WDTs to the non-timed-out state (see 3.2.1:3). The self-test is executed once each minor cycle, but alternates in its test of status for WDT1 and WDT2 as each watchdog timer is reset in alternate minor cycles. [IR759:591;81] This test shall read the status of an individual watchdog timer immediately before that watchdog timer is to be reset in its appropriate minor cycle. [IR759:591;82] This test shall be performed by both DCU A and DCU B.

A failure within this test occurs when the subject watchdog timer is found to be in a timed-out state prior to being reset.

[IR759:591;83] The response to a single failure of this test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.2 Periodic Self-Tests

These self-tests are performed at least once per major cycle but whose performance is independent of a particular event. Although they relate to the qualification/verification of electronic hardware, they are not directly associated with the performance of an engine control/monitoring event, but rather serve as periodic checks of the subject components. Execution of these tests within a major cycle is left to design discretion.

3.2.3:3.2.1 CIE Data MUX Self-Test

The CIE Data MUX Self-Test verifies that both the in-channel and cross-channel data MUXs can output both states of each bit onto the data bus. [IR759:1386;2] The self-test of the in-channel data MUXs shall be performed once per major cycle by both DCU A and DCU B. [IR759:3528;3] The self-test of the cross-channel data MUXs shall be performed once per major cycle by the in-control DCU only.

[IR759:591;85] The self-test shall read the two Channel A MUX Test Words and the two Channel B MUX Test Words (see Table XXXVII) to verify that each of the 16 MUX data bits can be toggled.

A failure within this self-test occurs when any one of the test words does not match its expected value. [IR759:2001;1] This self-test shall be considered to have failed after two successive failures (immediate reread).

3.2.3:3.2.1 CIE Data MUX Self-Test (Continued)

The response to failure of this self-test depends on whether the failure occurred on the in-channel data MUX or on the cross-channel data MUX. [IR759:591;87] The failure response for a cross-channel failure shall be to disqualify the cross-channel OE. [IR759:591;88] The failure response for an in-channel failure shall be to disqualify the in-channel DCU/CIE.

3.2.3:3.2.2 IE Address and Range Counters Self-Test

The IE Address and Range Counters Self-Test verifies that each DCU/CIE can load and read the in-channel IE address and range counters with data patterns that test both states of each bit in those registers. [IR759:591;89] This test shall be performed once per major cycle by both DCU A and DCU B. The standby DCU may perform the test at its convenience since manipulation of its address and range counters will not affect IE operations being conducted by the in-control DCU. [IR759:591;90] The in-control DCU shall perform the test only when an active IE input sequence is not in progress. [IR759:591;91] The DCU shall load the following address and range counter values into the appropriate registers, then read the corresponding data (see Table XXXVII) to verify the expected value. [IR759:591;92] The following set of data shall be used as test values on alternate major cycles (see Figure 18).

	IE Range Counter loaded value (bits 6-0)	IE Address Counter loaded value (bits 7-1)	Input Word expected value	
			(bits 14-8)	(bits 7-1)
Case 1	\$2A	\$55	\$2A	\$55
Case 2	\$55	\$2A	\$55	\$2A

A failure within this self-test occurs when the DCU does not read the expected value. [IR759:591;93] This self-test shall be considered to have failed after two successive failures (immediate retry). [IR759:591;94] The response to failure of this self-test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.2.3 Engine/Controller On/Off Devices Self-Test

The Engine/Controller On/Off Devices Self-Test verifies that the status of devices (that are controlled as on/off devices by means of the OE Storage Registers) agrees with their commanded state. This test will be considered an OE Self-Test because of the use of the OE in commanding and reading values, even though a failure of this Self-Test does not necessarily result in the disqualification of an OE. These devices consist of engine on/off devices (items a through c, below) and controller on/off devices (items d through j, below).

- (a) Igniters
- (b) Solenoids
- (c) Servoswitches
- (d) Group 1 Sensor Checkout Switches
- (e) Group 2 Propellant Drop Sensor Switches
- (f) Power Off Time Exceeded Indicator
- (g) OE 2khz Excitation
- (h) OE Solenoid Pull-In/Hold Voltage
- (i) PRC Overflow Test
- (j) Halt Exit Enable/Disable

[IR759:591;95] The self-test of the on/off devices shall be accomplished each major cycle by the in-control DCU reading the status of these devices (see Table XXXVII) and verifying that the status is equal to the commanded state.

[IR759:5006;1] Monitoring of the igniters shall be performed only in the Checkout and Start Preparation phases when the 2khz excitation has been selected. [IR759:5006;2] Igniter monitoring shall not begin until at least 18 msec after the 2khz excitation source is selected.

[IR759:2001;2] When any device has been commanded to change state, monitoring of the state of that device shall be suspended for the minimum delays shown below.

### 3.2.3:3.2.3 Engine/Controller On/Off Devices Self-Test (Continued)

<u>Commanded Function</u>	<u>Minimum Delay Required before Monitoring</u>
<u>Engine On/Off Devices</u>	
Igniter On or Off	55.0 msec
Solenoid	
Pull-In	10.0 msec
Pull-In/Hold to Off	6.0 msec
Servoswitch	
Fail-Op On	2.0 msec
Fail-Op Off	3.0 msec
Fail-Safe On	5.0 msec
Fail-Safe Off	1.0 msec

<u>Commanded Function</u>	<u>Minimum Delay Required before Monitoring</u>
<u>Controller On/Off Devices</u>	
Group 1 Sensor Checkout Switches	30.0 usec
Group 2 Propellant Drop Sensor Switches	30.0 usec
Power Off Time Exceeded Indicator	30.0 usec
OE 2khz Excitation	20.0 usec
OE Solenoid Pull-In/Hold Voltage	20.0 usec
PRC Overflow Test	30.0 usec
Halt Exit Enable/Disable	20.0 usec

A failure within this self-test occurs when the monitored state of any on/off device does not match that of the last commanded state. [IR759:3679;2] A device shall be considered to have failed after two successive failures (immediate reread). [IR759:1608;1] The response to failure of a particular device shall be per 3.2.4. The same Failure Identification Word will be reported for any non-disqualifying failures of an OE register. The Failure Identification Word identifies which On/Off register has failed, while the failure parameter identifies which device within the register has failed.

3.2.3:3.2.4 OE Servoactuator Model/Monitor Self-Test

The electronic servoactuator model monitors the performance of the servoactuator. If the servoactuator performance does not compare with the servoactuator model within a predetermined value, a Servoactuator Error Indication Interrupt (SEII) will be generated. The predetermined value is 6 percent of full scale OPOV servoactuator position for Channel A and 10 percent of full scale OPOV servoactuator position for Channel B. [IR759:2625;1] The monitor test of all qualified servoactuators shall be performed each major cycle by the in-control DCU except when SEII Monitoring is suspended (3.2.3:6.1.3).

The test is accomplished by positive and negative biasing of the servoactuator monitor summing junction.

The test sequence follows:

- (a) [IR759:5546;1] If both servoactuator channels are qualified the following shall occur:
  - (1) [IR759:5546;2] The servoactuator error indications shall be enabled in Channel B and disabled in Channel A.
  - (2) [IR759:5546;3] If an SEII occurs, Channel B servoactuators shall be disqualified per 3.2.1:6.4, regardless of the number of servoactuator error pending indications.
- (b) [IR759:591;101] The servoactuator error indications shall be disabled in the CIE. This is accomplished by using the Load CIE Interrupt Mask Register Two I/O instruction defined in Table XXXVIII to disable the indications via the mask register as defined in Table XXXIX.
- (c) [IR759:591;102] The positive or negative actuator monitor test shall be performed by loading both OE storage registers with the monitor test code defined in Table XXXIII and issuing transfer storage register I/O instructions for both OEs. The I/O instructions used to load and transfer the OE storage registers are defined in Table XXXVIII. [IR759:591;103] The OE storage registers shall not be loaded again until the monitor self-test is over. [IR759:591;104] The positive and negative actuator monitor tests shall be done in alternate major cycles.



3.2.3:3.2.4 OE Servoactuator Model/Monitor Self-Test  
(Continued)

- (d) [IR759:5566;1] After a 400 +150/-0 usec delay, all the qualified servoactuator error indications shall be enabled in the CIE. [IR759:591;106] If the SEII does not occur, the test shall be considered to have failed. [IR759:591;107] The response to failure of this test shall be to disqualify the DCU/CIE.
- (e) If the SEII does occur, the pending status of the servoactuator error indications is checked (see Table XXXVII). A failure within this self-test occurs when any enabled servoactuator does not have a corresponding servoactuator error indication pending.
- [IR759:3474;1] Fault detection shall be performed in the following order:
- (1) [IR759:3474;2] The response to the failure of all qualified servoactuators shall be detected by the Interrupt Decoder Self-Test (3.2.3:3.1.5).
  - (2) [IR759:3474;3] The response to the failure of one or more servoactuators (either the same servoactuator or different servoactuators) on each channel shall be to disqualify the DCU/CIE.
  - (3) [IR759:3474;4] The response to the failure of all servoactuators on the same channel shall be to disqualify the corresponding OE.
  - (4) [IR759:3474;5] The response to the failure of one or more (but not all) servoactuators on the same channel shall include disqualification of all the servoactuators on that channel. The complete failure response is dependent upon whether there had been a prior RVDT miscompare.
- (f) [IR759:591;110] The servoactuator error indications shall again be disabled as in step (b).  
[IR759:1386;6] The test shall be terminated by loading the OE storage registers with any value.
- (g) [IR759:5711;1] After an 800 +200/-200 usec delay, the SEII servoactuator error indications shall be cleared and returned to their nominal status per 3.2.3:6.1.3.

3.2.3:3.2.5 Interrupt Pending Self-Test

The Interrupt Pending Self-Test verifies that the DCU is responding properly to all pending interrupts.  
[IR759:591;113] The self-test shall be performed each major cycle by both DCU A and DCU B.

The test sequence follows:

- (a) [IR759:591;114] The interrupt pending status (see Table XXXVII) shall be read to ascertain if interrupts are pending.
- (b) [IR759:591;115] The current interrupt level shall be zero.
- (c) [IR759:591;116] The test shall delay by two CPU instructions to allow the DCU to service any pending interrupts.
- (d) [IR759:6245;1] After the delay, if any interrupts were pending in step (a), the interrupt pending status shall be reread to verify that pending interrupts have been serviced. If the interrupts are not pending, the interrupts were transients that were cleared within their corresponding service routines. If any interrupts are still pending, the interrupts were not cleared because their corresponding service routines were not executed.

A failure within this self-test occurs when the program that services a subject pending interrupt has not been executed.  
[IR759:591;118] The response to a single failure of this self-test shall be to disqualify the DCU/CIE that detected the error.

3.2.3:3.3 IE DPM Data Qualification/Verification Self-Tests

These self-tests directly relate to the testing of parameters input during the IE input sequence. [IR759:591;119] Unless specified to the contrary, these tests shall be performed following input of the entire IE DPM (see 3.2.1:2.1). [IR759:591;122] The tests shall be performed before any corresponding data parameters from the input are used for engine monitoring or control. [IR759:1386;7] All tests of this grouping shall be suspended for a failure detected in the IE Sequencer Self-Test (see 3.2.3:3.1.6) that requires temporary disqualification of all IE DPM data during the major cycle in which the error was detected. [IR759:2168;2] Furthermore, for the in-control DCU, the tests that are performed on data of the entire IE DPM conversion shall be performed in the following hierarchical manner:

- (a) IE Address and Data Bus Self-Test
- (b) Pulse Rate Converter Self-Tests and IE Analog to Digital Converter Self-Test in any order
- (c) All others in any order:

- OE RVDT/LVDT Excitation Power Supply Self-Test
- OE Digital to Analog Converters Self-Test
- PSE Internal Voltage Self-Test
- IE (VSPE) Channel C Power Supply Self-Test

[IR759:3528;4] If any aspect of the highest order test (a) fails, the program shall suspend all other self-tests in this IE DPM Data Qualification/Verification grouping from using the data of the affected IE until the next major cycle.

[IR759:3528;5] If any aspect of the IE Analog to Digital Converter Self-Test fails, the tests of the lowest order (c) shall be suspended from using the data of the affected IE during the major cycle in which the error was detected.

[IR759:2168;3] The standby DCU shall perform its designated tests regardless of the hierarchy.

3.2.3:3.3 IE DPM Data Qualification/Verification Self-Tests  
(Continued)

[IR759:2042;1] A common strike counter for IE failures shall be maintained for those ensuing self-tests that can disqualify an IE.

While a test is suspended:

- (d) [IR759:591;126] The corresponding data shall be considered invalid and shall not be used for engine control or monitoring purposes.
- (e) [IR759:591;127] The monitoring for individual data parameter failures shall be suspended.
- (f) [IR759:591;128] The corresponding strike counters for individual data parameters shall not be altered.

3.2.3:3.3.1 IE Address and Data Bus Self-Test

The IE Address and Data Bus Self-Test verifies that each IE data bit and IE address bit can be toggled. [IR759:591;129] This self-test shall be performed each major cycle in conjunction with the IE input sequence of 3.2.1:2.1. [IR759:591;130] This self-test shall be performed only by the in-control DCU.

Whenever an IE input sequence is requested by the DCU, complementary test patterns that toggle each bit in the IE data bus are written into specific IE DPM addresses. The combination of these addresses exercises all the address bits used by the IE.

The self-test reads these test patterns to verify that the expected values are received after an IE input sequence is completed.

The test sequence follows:

- (a) [IR759:4630;1] Prior to the IE input sequence being initiated, the following shall be performed:
  - (1) [IR759:1386;11] The IE DPM address locations specified for test words TW1A/TW1B, TW2A/TW2B, RC15/RC14 and RC19/RC18 shall be loaded with data patterns that are complementary to those that are written to these addresses during an IE input sequence.

3.2.3:3.3.1 IE Address and Data Bus Self-Test (Continued)

- (2) [IR759:4630;2] The contents of the specified address locations shall be read and compared with the loaded data to verify that they are equal.
  - (3) A failure within this test occurs when the value read at one of the specified address locations does not equal the loaded value. [IR759:4630;3] The response to a single failure of this test shall be to disqualify the DCU/CIE that detected the error.
- (b) [IR759:591;135] After the IE input sequence has been completed, the following shall be performed:
- (1) [IR759:1386;12] The IE DPM address locations associated with the parameter pairs of test words TW1A/TW1B, TW2A/TW2B, RC15/RC14, and RC19/RC18 shall be verified that they contain the expected values per Table XXX. The testing of RC15/RC14 and RC19/RC18 which is also necessary for the IE Analog to Digital Converter Self-Test of 3.2.3:3.3.3, is accomplished by this self-test.
  - (2) A failure within this test occurs when a parameter does not equal its expected value.
  - (3) [IR759:591;137] A single failure shall cause disqualification of all IE DPM data on that channel during the major cycle in which the error was detected. A single failure is defined as one or more parameter failures on the same channel.
  - (4) [IR759:591;138] If both parameters of any parameter pair should fail during the same IE input sequence, the response shall be to disqualify the DCU/CIE that detected the error.
  - (5) [IR759:591;139] If two successive failures occur for the same or differing parameters on the same IE channel, the response shall be to disqualify the IE in which the error was detected.

3.2.3:3.3.2 Pulse Rate Converter Self-Tests

The Pulse Rate Converter Self-Tests verify that specified PRCs update within a major cycle when pulse rate data is available for conversion within that time period. Pulse rate data is provided to the PRCs by speed sensors, flow sensors, and the 2khz RVDT/LVDT excitation frequency.

The IE input sequence will store new data into the IE DPM from a PRC only when the PRC has completed an update (new conversion). A new conversion, since the last input from that PRC, is indicated by the toggling of the MSB of the PRC input as stored in its IE DPM location.

[IR759:2042;2] A PRC Self-Test shall be performed, by the in-control DCU, in each major cycle during the specified monitoring period on the 2khz RVDT/LVDT Excitation Frequency, HPFP Shaft Speed, and Fuel Flowrate data. Other shaft speed data is input through PRCs, however, these values are used only for monitoring and do not affect controller component qualification nor do they affect engine control.

The 2khz RVDT/LVDT Excitation Frequency test is performed each major cycle since there should be no more than 1.0 msec before an update is detected. The frequency of update of the HPFP Shaft Speed and Fuel Flowrate PRCs is dependent upon engine operation. Since the PRC Self-Test for the HPFP Shaft Speed is performed in conjunction with Ignition Confirmation, the HPFP Shaft Speed may not update each major cycle, but it should update at least once during the monitoring period. The Fuel Flowrate PRC test is performed during periods when an update is expected each major cycle.

[IR759:2042;3] These tests shall verify that the MSB of applicable PRCs have toggled after each IE input sequence. A failure within these tests occurs when the MSB of a PRC has not toggled from its last conversion.

Because the PRC data for fuel flowrate and HPFP shaft speed is not updated each major cycle, such data could be out-of-date in the IE DPM when an IE input sequence is requested following any disruption of the PRCs. [IR759:5847;1] After the first input sequence following a disruption of the PRCs, the Operational Program shall assume that the state of the toggle bit is correct for the PRCs in the IE DPM, but will not use the data until the bit is toggled on an ensuing IE input sequence for the following disruptions:

- (a) Sensor Checkout
- (b) Suspension because of failure in IE Sequencer or IE Address and Data Bus Self-Test of 3.2.3:3.1.6 and 3.2.3:3.3.1 respectively
- (c) Execution of a Major Cycle Restart.

3.2.3:3.3.2 Pulse Rate Converter Self-Tests (Continued)

[IR759:5501;2] HPFP shaft speed data from the first input sequence following the disruption shall be used for ignition confirmation qualification monitoring.

The sensors being tested are as follows:

2khz RVDT/LVDT Excitation Frequency

TRCA/TRCB

HPFP Shaft Speed Sensors

N2A/N2B

Fuel Flowrate Sensors

Q1A1/Q1B1, Q1A2/Q1B2

3.2.3:3.3.2:1 2khz RVDT/LVDT Excitation Frequency

[IR759:3280;5] For the 2khz RVDT/LVDT Excitation Frequency, the test shall be performed during the following conditions:

- (a) When the source of the 2khz excitation has been selected and the OE Power Control Switch has been turned on in the OE being monitored.
- (b) When at least 4 msec have elapsed between commanding on the 2khz RVDT/LVDT power supply and input of these parameters.
- (c) When at least 1.75 msec has elapsed between commanding a change of excitation source and input of these parameters.

3.2.3:3.3.2:1 2khz RVDT/LVDT Excitation Frequency (Continued)

[IR759:2042;5] If the MSB for the 2khz RVDT/LVDT Excitation Frequency parameter did not toggle for two successive major cycles, the response shall be to disqualify the OE in which the error was detected. [IR759:2042;6] A separate OE strike counter shall be retained for this self-test.

3.2.3:3.3.2:2 HPFP Shaft Speed Sensors

[IR759:2042;7] For the HPFP Shaft Speed, the test shall be performed when the ignition confirmation shaft speed test is being performed, per Table XVII. [IR759:2042;8] When this test is performed, it shall precede all other HPFP Shaft Speed qualification tests.

[IR759:2042;9] A single failure of the test shall cause temporary disqualification of that sensor's data during the major cycle in which the error was detected.

[IR759:2042;10] Failure of the MSB to toggle for three successive major cycles shall cause permanent disqualification of the sensor.

3.2.3:3.3.2:3 Fuel Flowrate Sensors

[IR759:2042;11] For the Fuel Flowrate, the test shall be performed when the measured MCC Pc is at or above 49% RPL. [IR759:5522;1] When this test is performed it shall precede the Fuel Flowrate Sensor Qualification Test. [IR759:2042;13] A single failure of the test shall cause temporary disqualification of that sensor's data during the major cycle in which the error was detected.

[IR759:2042;14] Failure of the MSB to toggle for three successive major cycles shall cause permanent disqualification of the sensor.

3.2.3:3.3.3 IE Analog to Digital Converter Self-Test

The IE Analog to Digital Converter Self-Test verifies the conversion accuracy of the A/D Converter. [IR759:591;145] This self-test shall be performed each major cycle in conjunction with the IE input sequence of 3.2.1:2.1. [IR759:2168;7] This self-test shall be performed by DCU A and DCU B.



### 3.2.3:3.3.3 IE Analog to Digital Converter Self-Test (Continued)

The test sequence follows:

(a) [IR759:2168;8] Prior to the IE input sequence being initiated, the IE DPM address locations specified for RC05/RC04 and RC21/RC20 shall be loaded with the value \$8000, and RC09/RC08 with the value \$7FFF by the in-control DCU only.

(b) [IR759:591;148] After the IE input sequence has been completed, the following shall be performed:

(1) [IR759:4381;2] The following parameters shall be verified to be within the limits as shown below.

<u>Parameter</u>	<u>Min Limit (VDC)</u>	<u>Max Limit (VDC)</u>
RC09/RC08	\$FE48 (-0.0004)	\$01C8 (0.0005)
RC21/RC20	\$FE48 (-0.0004)	\$01C8 (0.0005)
IE1A/IE1B	\$AA08 (-10.1)	\$ABA8 (-9.9)
IE2A/IE2B	\$5298 (9.7)	\$57B8 (10.3)
RC05/RC04	\$FED8 (-0.0003)	\$0138 (0.0003)
RC03/RC02	\$6038 (0.025)	\$6238 (0.026)
RC07/RC06	Min Memory	Max Memory
RC13/RC12	\$5DF8 (0.142)	\$5FF8 (0.145)
RC17/RC16	\$5DF8 (0.142)	\$5FF8 (0.145)

The testing of RC15/RC14 and RC19/RC18 which is necessary for this self-test is accomplished by the IE Address and Data Bus Self-Test of 3.2.3:3.3.1.

(2) A failure within this test occurs when a parameter is out of limits.

(3) [IR759:591;150] A single failure shall cause disqualification of all IE DPM data on that channel during the major cycle in which the error was detected. A single failure is defined as one or more parameter failures on the same channel.

3.2.3:3.3.3 IE Analog to Digital Converter Self-Test  
(Continued)

- (4) [IR759:2168;10] If two successive failures occur for the same or differing parameters on the same IE channel, the failure response for the in-control DCU shall be to disqualify the IE in which the error was detected.
- (5) [IR759:2168;11] For the standby DCU all failures on the same channel shall be considered as single failures with only the IE DPM data being disqualified.

3.2.3:3.3.4 OE RVDT/LVDT Excitation Power Supply Self-Test

The OE RVDT/LVDT Excitation Power Supply Self-Test verifies that the OE RVDT/LVDT excitation power supply outputs track the OE On/Off Register 2A/2B OE 2khz Excitation commands as shown in Table XXXI. [IR759:591;152] This self-test shall be performed each major cycle by the in-control DCU.

[IR759:4381;3] The test shall compare the monitored frequency parameters (TRCA/TRCB) and amplitude parameters (FRVA/FRVB) of the excitation voltage in the IE DPM to the limits listed below when the source of the 2khz excitation has been selected and the OE Power Control Switch has been turned on in the OE being monitored.

<u>Parameter</u>	<u>Min Limit</u>	<u>Max Limit</u>
FRVA/FRVB	\$6F78 (19.1 Vpp)	\$7A18 (20.9 Vpp)
TRCA/TRCB	\$01F0 (2016 pps)	\$01F7 (1988 pps)

[IR759:3280;7] Verification of the parameters shall, however, be suspended following RVDT/LVDT power on, or change of excitation source as follows:

<u>Event</u>	<u>Parameter</u>	<u>Minimum Delay from Event Output to IE Input of Parameter</u>
Power on	FRVA/FRVB	10.0 msec
	TRCA/TRCB	4.0 msec
Change of Source	FRVA/FRVB	1.5 msec
	TRCA/TRCB	1.75 msec

### 3.2.3:3.3.4 OE RVDT/LVDT Excitation Power Supply Self-Test (Continued)

The OE RVDT/LVDT excitation power supply will be set (power on) whenever the OE Power Control Switch is turned on as a result of exiting PROM, power recovery, DCU B takeover, or subsequent to Controller Checkout.

[IR759:3280;8] In addition, the first set of TRCA/TRCB parameters that are input following a power on or change of source shall be discarded.

A failure within this test occurs when a parameter is out of limits. [IR759:2092;1] The first such failure shall cause RVDT/LVDT excitation to be temporarily disqualified for the affected channel. [IR759:2092;2] If the channel temporarily disqualified is the controlling channel, all fail-safe servoswitches shall be deenergized, and all actuator position commands shall be retained. [IR759:2092;3] Any actuator command ramping function in effect per 3.2.3:2.3.6 and Tables X, XI, XII, XIII, XIV, XV, XXIV, XXV, shall be suspended. [IR759:2092;4] When excitation is confirmed as qualified for a controlling channel, the following shall be performed in the order specified:

- (a) [IR759:2092;5] New actuator position commands shall be determined. [IR759:2092;6] If an actuator ramp rate is in effect, the new actuator position command shall be calculated by applying the ramp rate to the current commanded position. [IR759:2092;7] Otherwise, actuator position commands shall be calculated according to the applicable control for the current engine phase and mode.
- (b) [IR759:2092;8] New actuator position commands shall be issued to all servoactuators.
- (c) [IR759:2092;9] Fail-safe servoswitches shall be commanded to the state described in Servoswitch and Solenoid Data processing (3.2.3:6.3).

[IR759:591;155] This self-test shall be considered to have failed after two successive failures on the same parameter. [IR759:591;156] The response to failure of this self-test shall be to disqualify the OE in which the error was detected. [IR759:2092;10] Then fail-safe servoswitches shall be commanded for the remaining qualified channel as per 3.2.3:6.3.

SEII monitoring will be suspended for all servoactuator channels whenever RVDT/LVDT excitation is deactivated (3.2.3:6.1.3).

3.2.3:3.3.5 OE Digital to Analog Converters Self-Test

The OE D/A converters latch the DCU digital servovalve commands and convert them into the equivalent analog values. The OE Digital to Analog Converters Self-Test verifies:

- (a) That each D/A output voltage level is equal to its last commanded value.
- (b) That the command decoder addresses the correct D/A by proper decoding of the 4 LSBs of the OE Storage Register. If the decoder operation is in error, the command verified at the storage register will be improperly transferred. The transfer will either not be implemented or will be made to the wrong destination. This incorrect transfer may be detected when the D/A output is observed to be at other than the commanded level.

[IR759:591;162] This test shall be performed by the in-control DCU subsequent to the processing that issues the servovalve commands. This test will be performed before the RVDT Comparison Test (3.2.3:6.1.4) to prevent entry into Hydraulic Lockup because of a disqualified IE causing an RVDT miscompare followed immediately by a D/A converter failure.

The test sequence follows:

- (c) [IR759:591;163] After a delay of at least 100 usec from the transfer of the last servovalve command to the D/A via the OE Storage Register, the IE input sequence shall be initiated for the D/A outputs. [IR759:591;164] Spare servovalve commands shall not be input and thus are excluded from this self-test.
- (d) [IR759:4315;1] Each D/A output parameter of Group 4 (see Table XXX) stored in the IE DPM, excluding any spares, shall be compared to its corresponding LDA input value (Figure 7).

[IR759:4315;2] A failure within this self-test shall occur when the difference between D/A output and its corresponding LDA input is not within +/-51. This tolerance is 1.5% of OPOV full range from -5% to 105%.

3.2.3:3.3.5 OE Digital to Analog Converters Self-Test  
(Continued)

- (e) [IR759:2001;5] If a failure is detected, an immediate reread shall be performed by repeating step (c) for all servovalve commands for which a failure occurred.
- (f) [IR759:591;167] If, following the IE input sequence associated with step (e), an input parameter has a second successive failure, the failure response shall include disqualification of all servoactuators on the channel which had the detected failure. The complete failure response is dependent upon whether there had been a prior RVDT miscompare during a previous major cycle.

3.2.3:3.3.6 PSE Internal Voltages Self-Test

The PSE Internal Voltages Self-Test verifies that PSE internal voltages are within limits.

[IR759:3528;7] This self-test shall be performed each major cycle by the in-control DCU only.

[IR759:591;182] This self-test shall compare the monitored voltage parameter (P/S+5A or P/S+5B) in the IE DPM to the limits listed below.

<u>Minimum Limit</u>	<u>Maximum Limit</u>
\$5478 (4.4 Vdc)	\$6BE8 (5.6 Vdc)

[IR759:3528;8] DCU A shall test both the in-channel parameter P/S+5A and the cross-channel parameter P/S+5B. [IR759:3528;9] Only when DCU B is in control shall DCU B test its in-channel parameter P/S+5B. A failure within this self-test occurs when a parameter is out of limits. [IR759:591;184] This self-test shall be considered to have failed after two successive failures on the same parameter. The response to failure of this self-test depends on whether the failure occurred on the in-channel PSE or on the cross-channel PSE. [IR759:3528;10] The failure response for an in-channel failure shall be to disqualify the DCU/CIE that detected the error. [IR759:3528;11] The failure response for a cross-channel failure shall be to report the failure (FID 20).

3.2.3:3.3.7 IE (VSPE) Channel C Power Supply Self-Test

The IE (VSPE) Channel C Power Supply Self-Test verifies that the Channel C power used by the Channel C VSPE is within limits. See Figure 19 for the relationship between accelerometers, VSPE and the Channel C power supplies.

[IR760:6239;1] The IE (VSPE) Channel C Power Supply Self-Test shall be performed each major cycle by the in-control DCU, but shall be suspended when the FASCOS Bypass option is in effect (3.2.5:2). [IR761:2890;1] This self-test shall compare the IE (VSPE) Channel C Power Supply's +15 Vdc (IE3CA/IE3CB) and -15 Vdc (IE4CA/IE4CB) parameters against the limits given below. The check on the limits also serves as a support function of the PSE Logic/Redundancy Tests.

<u>Parameter</u>	<u>Minimum Limit (Vdc)</u>	<u>Maximum Limit (Vdc)</u>
IE3CA/IE3CB	\$5378 (14.2)	\$5C68 (15.8)
IE4CA/IE4CB	\$A398 (-15.8)	\$AC88 (-14.2)

[IR762:1642;1] Failure of this test shall occur when a parameter is out of limits. [IR762:1642;2] If two successive failures occur for the same parameter, that parameter shall be permanently disqualified. [IR762:1642;3] If at least one channel of each voltage is qualified, the Channel C Power Supply voltage shall be qualified. [IR762:1642;4] If both channels of a given voltage are temporarily disqualified, or one is temporarily disqualified and the other is permanently disqualified, the Channel C vibration input parameters (V1CA, V1CB, V2CA, and V2CB) shall be temporarily disqualified during the major cycle in which the error was detected. [IR762:1642;5] If both channels of either voltage are permanently disqualified, the Channel C vibration sensors shall be permanently disqualified and this test shall be suspended.

3.2.3:4 Engine Sensor Data Processing

This section describes the requirements to be satisfied in processing sensor input parameters and generating responses to detected malfunctions or failures associated with the SSME sensor inputs. For each parameter there is either a single sensor, a sensor on each channel, or two sensors on each channel.

3.2.3:4 Engine Sensor Data Processing (Continued)

Included in sensor data processing is data scaling and the monitoring functions of data qualification and disqualification, shutdown limit checking, control parameter computation, and setting of control values. The monitoring periods and limits are specified in Table XVII.

For each sensor listed in 3.2.3:4.1, data scaling is performed to obtain physical units. Qualification of the data is accomplished by tests and criteria specified in 3.2.3:4.2, wherein sensor and channel values are either qualified for use, or disqualified.

Temporary disqualification will occur upon failure of a monitoring test, per 3.2.3:4.3.1, while permanent disqualification will occur upon a specified number of consecutive failures, per 3.2.3:4.3.2. The inputs from a temporarily or permanently disqualified sensor or IE will not be used for any processing other than scaling, VDT reporting, and self-qualification, per 3.2.3:4.3.

Control parameter channel values are computed according to 3.2.3:4.4.1, and control values obtained, per 3.2.3:4.4.2.

3.2.3:4.1 Sensor Input Data Scaling

[IR764:6164;1] Independent of sensor or IE qualification, the IE DPM input data from each channel of the following sensors (excluding spares) shall be scaled each major cycle, i.e., converted into a number representing the physical units of the measured parameter, per Table XXVIII:

- All Pressures
- All Temperatures
- All Shaft Speeds
- All Fuel Flowrates
- All Actuator Positions
- All Valve Positions
- All High Pressure Pump Vibrations
- Both Input Power Bus Voltages
- All Servovalve Currents

During Actuator Checkout these additional parameters must be scaled for use in the Actuator Checkout VDT:

- OE +29 Voltage on Channel A
- OE +24 Voltage on Channel B
- Both RVDT/LVDT Excitation Amplitudes

3.2.3:4.1 Sensor Input Data Scaling (Continued)

Implicit in the conversion of the value in Dual Port Memory to physical units are sensor characteristics, analog to digital conversion, and Controller Internal scale factors. Table XXVII relates physical parameter measurement to sensor output.

3.2.3:4.2 Sensor Input Data Qualification

Sensors and/or sensor channels are qualified for specific functions. With the exception of MCC Pc in Shutdown Limit Monitoring, if a parameter is used for more than one function the qualification criteria for the sensor and/or sensor channel are identical for each function. In general, with the noted exception, qualification of a sensor or sensor channel for a particular function will qualify that sensor or sensor channel for all functions.

This paragraph specifies qualification requirements for:

(a) Control Parameters

- (1) Main Combustion Chamber Pressure (MCC Pc)
- (2) Fuel Flowrate
- (3) LPFP Discharge Pressure
- (4) LPFP Discharge Temperature

(b) Shutdown Limit Monitor Parameters

- (1) Main Combustion Chamber Pressure (MCC Pc)
- (2) HPFT Discharge Temperature
- (3) HPOT Discharge Temperature
- (4) HPOP IMSL Purge Pressure
- (5) HPOT Secondary Seal Cavity Pressure
- (6) HPFP Coolant Liner Pressure
- (7) Fuel Preburner Shutdown Purge Pressure
- (8) Oxidizer Preburner Shutdown Purge Pressure

(c) Ignition Confirmation Parameters

- (1) Main Combustion Chamber Pressure (MCC Pc)
- (2) Antiflood Valve
- (3) HPFP Shaft Speed

(d) Propellant Drop Parameters

- (1) LPFP Discharge Temperature
- (2) Preburner Pump Discharge Temperature
- (3) Fuel Flowrate



3.2.3:4.2 Sensor Input Data Qualification (Continued)

(e) Engine Ready Parameters

- (1) LPFP Discharge Pressure
- (2) LPFP Discharge Temperature
- (3) Preburner Pump Discharge Temperature
- (4) LPOP Discharge Pressure
- (5) Emergency Shutdown Pressure
- (6) Fuel Preburner S/D Purge Pressure
- (7) Oxidizer Preburner S/D Purge Pressure
- (8) MOV Hydraulic Temperature
- (9) MFV Hydraulic Temperature

(f) Pogo GOX Flow Check Parameters

- (1) Pogo Precharge Pressure

(g) Vibration Limit Monitoring Parameters

- (1) HPFP Acceleration
- (2) HPOP Acceleration

(h) Backdoor Purge Initiation Monitoring Parameters

- (1) HPOP IMSL Purge Pressure
- (2) Fuel Preburner Shutdown Purge Pressure
- (3) Oxidizer Preburner Shutdown Purge Pressure
- (4) Pogo Precharge Pressure

(i) RVDT Monitoring Parameters

- (1) HPFT Discharge Temperatures
- (2) HPOT Discharge Temperatures
- (3) Actuator Positions

(j) Purge and Ancillary System Monitoring Parameters

- (1) Emergency Shutdown Pressure
- (2) Fuel Bleed Valve Position
- (3) Oxidizer Bleed Valve Position
- (4) Pogo Recirculation Isolation Valve Position
- (5) Antiflood Valve Position
- (6) Fuel System Purge Pressure
- (7) HPOP IMSL Purge Pressure
- (8) Pogo Precharge Pressure
- (9) MOV Hydraulic Temperature
- (10) MFV Hydraulic Temperature

3.2.3:4.2 Sensor Input Data Qualification (Continued)

- (k) GN2/He Purge Monitoring Parameter
  - (1) HPOP IMSL Purge Pressure
- (l) MCC LOX Dome Temperature Monitoring Parameter
  - (1) MCC LOX Dome Temperature
- (m) Preburner Pump Discharge Temperature Sensor Integrity Monitoring Parameter
  - (1) Preburner Pump Discharge Temperature
- (n) Actuator Settling Check Parameters
  - (1) MFV Actuator Positions
  - (2) MOV Actuator Positions
  - (3) FPOV Actuator Positions
  - (4) OPOV Actuator Positions
- (o) Cold Junction Temperature Monitoring Parameter
  - (1) Cold Junction Temperature

3.2.3:4.2.1 Sensor Input Data Qualification General Rules

- (a) [IR764:6164;2] Qualification of data for a particular function from those sensors listed in 3.2.3:4.2 that have not been permanently disqualified for that function shall be accomplished per the criteria of 3.2.3:4.2.2 through 3.2.3:4.2.16. Also, no data qualification will be performed for any position sensors associated with a disqualified OE.
- (b) No sensor data qualification or failure response will be performed during the Sensor Checkout Test (3.2.3:2.3.1).
- (c) [IR764:2218;2] Failure of a qualification test for a particular function shall cause the affected sensor or channel to be temporarily or permanently disqualified for that parameter for that function.
- (d) [IR764:2218;3] A single successful test shall restore the qualified status of an affected sensor or channel for associated functions.

3.2.3:4.2.1 Sensor Input Data Qualification General Rules  
(Continued)

(e) Because the PRC data for Fuel Flowrate and the HPFP shaft speed may not be updated each major cycle, such data could be out of date following any disruption of the PRCs. [IR767:5501;1] Therefore, subsequent to any of the conditions (1) through (6), below, resulting in disruption of the PRCs, Fuel Flowrate and the HPFP shaft speed data shall not be used until the associated PRC update bits toggle in succeeding IE DPM updates except as noted in 3.2.3:3.3.2, Pulse Rate Converter Self-Tests.

- (1) Exit PROM command
- (2) Controller Checkout
- (3) Recovery from a power transient on either channel
- (4) Sensor Checkout
- (5) Change of excitation source
- (6) Suspension because of failure in IE Sequencer or IE Address and Data Bus Self-Test of 3.2.3:3.1.6 and 3.2.3:3.3.1 respectively.

3.2.3:4.2.2 Control Parameter Qualification

[IR767:5895;1] Sensor input data for each set of control parameters shall be qualified for use in computing control values (3.2.3:4.4.2) during the periods specified in Table XVII, according to the criteria given below, as detailed in Table XVII.

(a) MCC Pc Sensors

There are two MCC Pc sensors on each channel. A channel is qualified for usage of MCC Pc values by meeting the criteria of the tests below.

(1) Intra-channel Comparison Test

The difference of the values of the two MCC Pc sensors on each channel will be verified to be within a fixed value.

(2) Channel Reasonableness Tests

The Fixed Limits and Pc Reference tests comprise the MCC Pc Channel Reasonableness tests. The average of the two MCC Pc sensors on a channel will be verified to either be within fixed limits, or be within limits that are a function of Pc Reference.

3.2.3:4.2.2 Control Parameter Qualification (Continued)

- (3) [IR774:1608;1] Failure of test (1) or (2) shall temporarily or permanently disqualify the channel for MCC Pc monitoring, according to the criteria of 3.2.3:4.3.

[IR774:5501;1] During Ignition Confirmation, a temporary IE strike shall be considered a strike against MCC Pc control qualification.

(b) Fuel Flowrate Sensors

There are two Fuel Flowrate sensors on each channel. Individual sensors are qualified by meeting the criteria of (1) and (2), below.

(1) PRC Self-Test

Each Fuel Flowrate sensor will be verified to have updated each major cycle when the measured MCC Pc is at or above 49% RPL per 3.2.3:3.3.2:3. This assures only updated values are used. When this test is executed it will precede the Sensor Qualification Test.

(2) Sensor Qualification Test

Each Fuel Flowrate sensor on each channel will be verified to be within limits that are a function of a computed volumetric fuel flowrate reference value, Q reference. [IR782:1608;1] Individual Fuel Flowrate sensors failing this test shall be temporarily or permanently disqualified, according to the criteria of 3.2.3:4.3. [IR785:5522;1] The Sensor Qualification Test shall only be performed on a sensor if it has been updated. During the major cycles in which no update is detected the Sensor Qualification Test will be bypassed.

[IR790:5880;1] In Checkout Standby and Start Preparation phases, all temporary strikes against a fuel flowrate sensor shall be cancelled if eight major cycles of monitoring for updates have elapsed without an update being detected.

[IR790:5880;2] Upon acceptance of a Start Enable command, all failures against this test shall be removed if a sensor is temporarily disqualified as a result of this test.

3.2.3:4.2.2 Control Parameter Qualification (Continued)

(c) LPFP Discharge Pressure and Temperature Sensors

There is one LPFP Discharge Pressure sensor and one LPFP Discharge Temperature sensor on each channel. These sensors are qualified according to the following criteria.

(1) LPFP Discharge Pressure and Temperature Sensor Qualification Tests

The value of each sensor will be verified to be within fixed (reasonableness) limits.

3.2.3:4.2.3 Shutdown Limit Parameter Qualification

[IR792:6262;1] Sensor input data for each Shutdown Limit parameter shall be qualified for use in Shutdown Limit (Redline) Monitoring (3.2.3:5.3) during the periods specified in Table XVII, according to the criteria given below, as detailed in Table XVII.

(a) MCC Pc Sensor Channels

A channel is qualified for usage of the values of its two MCC Pc sensors by meeting the criteria of the following tests:

(1) Shutdown Limit Monitoring Intra-Channel Comparison Test

The difference of the values of the two MCC Pc sensors on each channel will be verified to be within a specified value.

(2) Shutdown Limit Monitoring Reasonableness Test

The average of the two MCC Pc sensor values on a channel will be verified to be within specified limits.

(b) HPOT and HPFT Discharge Temperature Sensors

There are two HPOT Discharge Temperature sensors and two HPFT Discharge Temperature sensors on each channel. [IR792:6164;2] A sensor is qualified for usage of its value by meeting the criteria of the ensuing tests which shall be performed in the following order:

3.2.3:4.2.3 Shutdown Limit Parameter Qualification  
(Continued)

(1) Shutdown Limit Monitoring Individual Sensor Test

Each HPOT Discharge Temperature sensor value and HPFT Discharge Temperature sensor value will be verified to be within specified limits during Start Preparation and not exceeding a specified upper limit during Start or Mainstage.

(2) Shutdown Limit Monitoring Intra-Channel Comparison Test

[IR792:6164;3] The intra-channel comparison test is a lower limit check which shall be performed if both sensors on a channel have passed the previous individual sensor test. [IR792:6164;4] If the difference of the values of the two sensors on a channel is not within a specified limit, the lower reading sensor shall be specified as the sensor that failed the check.

(3) Shutdown Limit Monitoring Inter-Channel Comparison Test

[IR792:6164;5] The inter-channel comparison test is a lower limit check which shall be performed only when one sensor on a channel has been temporarily or permanently disqualified and there is at least one qualified sensor on the other channel. The comparison test must include the bias that exists between the channels. The nominal biases are the delta values in Table XVII.

[IR792:6164;6] If only one sensor has been temporarily or permanently disqualified, the single qualified sensor value on the channel shall be verified to be within a specified limit of the average value of the two qualified sensors on the other channel, adjusted for the bias between channels. [IR792:6164;7] If the limit check is unsuccessful, the single sensor shall be specified as the sensor that failed the check.

3.2.3:4.2.3 Shutdown Limit Parameter Qualification  
(Continued)

[IR792:6164;8] If both channels have one sensor temporarily or permanently disqualified, the difference of the values of the remaining qualified sensors shall be verified to be within a specified limit, adjusted for the bias between channels. [IR792:6164;9] If the limit check is unsuccessful, the lower reading sensor shall be specified as the sensor that failed the check.

[IR792:6164;10] Failure of test (1), (2), or (3) shall temporarily or permanently disqualify the specified sensor according to the criteria of 3.2.3:4.3.

(c) Other Shutdown Limit Monitor Sensors

HPOP IMSL Purge Pressure, HPOT Secondary Seal Cavity Pressure, and HPFP Coolant Liner Pressure are monitored by one sensor on each channel. Fuel Preburner Shutdown Purge Pressure and Oxidizer Preburner Shutdown Purge Pressure are each monitored by a single sensor. Each sensor is individually qualified for use as a Shutdown Limit parameter if within the limits specified in the respective Sensor Qualification Test in Table XVII.

3.2.3:4.2.4 Ignition Confirmation Parameter Qualification

[IR793:2042;1] Sensor input data for MCC Pc, Antiflood Valve (AFV) Position, and HPFP Shaft Speed shall be qualified for use in Ignition Confirmation commencing respectively at the times specified in Table XVII, according to the criteria below.

[IR793:2218;2] Qualification for Ignition Confirmation shall continue until the parameter passes the ignition confirmation criteria (3.2.3:5.2) once during each three major cycle ignition confirmation monitoring period, or until three failures occur. [IR793:5501;1] A temporary disqualification of an IE shall be considered a strike against ignition confirmation qualification.

(a) MCC Pc Sensor Channels

The MCC Pc channel value (the average of the values of a channel's two MCC Pc sensors) will pass the MCC Pc Intra-Channel Qualification test and the Fixed Limits and Pc Ref Channel Qualification tests of Table XVII. Performance of the tests and disqualifications will be as specified in 3.2.3:4.2.2 (a) (1) through (3).

(b) HPFP Shaft Speed Sensors

The HPFP Shaft Speed sensors on each channel will be verified to have updated per 3.2.3:3.3.2:2, and will then be verified to be within their respective Ignition Confirmation sensor qualification limits, as per Table XVII. [IR793:2042;2] An HPFP Shaft Speed sensor shall be considered to have failed qualification for Ignition Confirmation for that major cycle if the HPFP Shaft Speed PRC does not update, or if the PRC does update and the HPFP Shaft Speed value is not within qualification limits.

(c) AFV Position Sensors

The AFV Position sensor on each channel will be verified to be within the limits as specified in Table XVII for their respective Ignition Confirmation Sensor Qualification tests. [IR793:5501;2] AFV data from the first IE input sequence following power recovery on either channel shall be used for ignition confirmation qualification. [IR793:5501;3] A temporary disqualification of an OE shall be considered a strike against ignition confirmation qualification.



3.2.3:4.2.5 Propellant Drop Monitoring Parameter Qualification

[IR794:2218;1] If there is no power loss of the associated power source, and the associated IE is qualified, input data from the LPFP Discharge Temperature sensor and Preburner Pump Discharge Temperature sensor on each channel shall always be considered to be qualified for use in Propellant Drop Monitoring (3.2.3:2.1).

[IR794:5522;1] Input data from the four Fuel Flowrate sensors shall be qualified for use in Propellant Drop Monitoring per 3.2.3:4.2.2.

3.2.3:4.2.6 Engine Ready Parameter Qualification

[IR794:2218;2] If there is no power loss of the associated power source, and the associated IE is qualified, input data from the Preburner Pump Discharge Temperature, LPOP Discharge Pressure, Emergency Shutdown Pressure, MOV Hydraulic Temperature and MFV Hydraulic Temperature sensors on each channel shall always be considered to be qualified for use in Engine Ready Monitoring (3.2.3:5.1).

[IR794:3407;1] Input data from the single Fuel Preburner Shutdown Purge Pressure sensor and the Oxidizer Preburner Shutdown Purge Pressure sensor, as well as input data from the LPFP Discharge Pressure and LPFP Discharge Temperature sensors on each channel shall be qualified for use in Engine Ready Monitoring at the times specified in Table XVII, if within the limits specified in Table XVII.

3.2.3:4.2.7 Pogo GOX Flow Check Parameter Qualification

[IR794:2218;3] Input data from the two Pogo Precharge Pressure sensors shall be qualified for use in the Pogo GOX Flow check commencing at the times specified in Table XVII by being within the limits specified in the Pogo GOX Flow Check Qualification Test in Table XVII.

[IR794:2218;4] Qualification for the Pogo GOX Flow Check shall continue until the parameter passes the Pogo GOX Flow Check criterion (3.2.3:6.5), or until three failures occur.

[IR794:5501;1] A temporary disqualification of an IE shall be considered a strike against the Pogo GOX Flow Check qualification. Passage or failure will occur within the three major cycle duration of the Pogo GOX Flow Check.

3.2.3:4.2.8 Vibration Limit Parameter Qualification

[IR795:6239;1] Vibration Limit Monitor Sensors shall be qualified according to the criteria below, for use in FASCOS Limit Monitoring (3.2.3:5.4), except when the FASCOS Bypass option is in effect (3.2.5:2). [IR795:6239;2] If the FASCOS Bypass option is in effect, each vibration sensor shall be assumed to be qualified until its possible disqualification by an ensuing power or IE failure. In addition, each vibration sensor will continue to be scaled only for reporting in the VDT.

(a) IE (VSPE) Channel C Power Supply Self-Test.

This Self-Test of 3.2.3:3.3.7 detects failures of the Channel C VSPE power (+/- 15 VDC). A failure of this test may either temporarily or permanently disqualify the Channel C HPPF and HPOP vibration sensors (V1CA, V1CB, V2CA and V2CB).

(b) Vibration Sensor Qualification Test

[IR795:3407;1] The value of each vibration sensor shall be verified to be within the limits specified in Table XVII.

[IR795:5344;1] This test shall be suspended on all vibration channels for three major cycles after a recoverable power transient on either DCU channel. [IR795:5344;2] Suspension shall result in resetting the strike counters for the qualification monitors.

[IR795:2218;2] This test shall be bypassed for the Channel C vibration sensors if they are temporarily or permanently disqualified by the IE (VSPE) Channel C Power Supply Self-Test.

3.2.3:4.2.9 Backdoor Purge Initiation Monitoring Parameter Qualification

[IR795:3407;2] Input data from HPOP IMSL Purge Pressure, Fuel Preburner Shutdown Purge Pressure, Oxidizer Preburner Shutdown Purge Pressure, and Pogo Precharge Purge Pressure sensors shall be qualified for use in Backdoor Purge Initiation Monitoring (3.2.3:5.5) during the times specified in Table XVII, if the applicable sensors are within the limits specified in Table XVII.

3.2.3:4.2.10 RVDT Monitoring Parameter Qualification

[IR795:3408;1] Input data from the five Channel A Actuator Position sensors and the five Channel B Actuator Position sensors shall be considered to be qualified for use in RVDT Comparison Test (3.2.3:6.1.4), or the Channel B RVDT Monitoring in Start Preparation (3.2.3:6.1.5), if the

### 3.2.3:4.2.10 RVDT Monitoring Parameter Qualification (Continued)

respective actuators are qualified. [IR795:3407;3] Input data from HPFT Discharge Temperature and HPOT Discharge Temperature sensors shall be qualified for use in RVDT Comparison Test during the times specified in 3.2.3:6.1.4 if applicable sensor values are within the limits specified in Table XVII.

### 3.2.3:4.2.11 Purge and Ancillary System Monitoring Parameter Qualification

[IR795:3326;1] If there is no power loss of the associated power source, and the associated IE is qualified, input data from Emergency Shutdown Pressure, Fuel System Purge Pressure, MOV Hydraulic Temperature, and MFV Hydraulic Temperature sensors shall always be considered to be qualified for use in Purge and Ancillary System Monitoring (3.2.3:6.4).

[IR795:3326;2] If there is no power loss of the associated power source, and the associated IE and OE are qualified, input data from the Fuel Bleed Valve Position, Oxidizer Bleed Valve Position, and the Pogo Recirculation Isolation Valve Position sensors shall always be considered to be qualified for use in Purge and Ancillary System Monitoring (3.2.3:6.4).

[IR795:4243;1] Input data from Antiflood Valve Position, HPOP IMSL Purge Pressure and Pogo Precharge Pressure sensors shall be qualified for use in Purge and Ancillary System Monitoring during the times specified in Table XVII, if within the limits specified in Table XVII.

### 3.2.3:4.2.12 GN2/He Purge Monitor Parameter Qualification

[IR795:3407;5] Input data from HPOP IMSL Purge Pressure sensors shall be qualified for use in GN2/He Purge Monitoring (3.2.3:6.6) during the times specified in Table XVII, if the applicable sensors are within the limits specified in Table XVII.

### 3.2.3:4.2.13 MCC LOX Dome Temperature Parameter Qualification

[IR795:3981;1] If there is no power loss on channel B and IE B is qualified, input data from the MCC LOX Dome Temperature shall always be considered to be qualified for use in MCC LOX Dome Temperature Monitoring (3.2.3:6.7).

### 3.2.3:4.2.14 Preburner Pump Discharge Temperature Sensor Integrity Monitor Parameter Qualification

[IR795:3070;1] If there is no power loss of the associated power source and the associated IE is qualified, input data from the Preburner Pump Discharge Temperature sensor channel shall always be considered to be qualified for use in Preburner Pump Discharge Temperature Sensor Integrity monitoring (3.2.3:6.8).

3.2.3:4.2.15 Actuator Settling Check Parameter Qualification

[IR795:3070;2] Input data from the MOV, MFV, FPOV, and OPOV Channel A Actuator Position sensors and the MOV, MFV, FPOV, and OPOV Channel B Actuator Position sensors shall be considered qualified for use in the Actuator Settling Check if the respective actuators are qualified.

3.2.3:4.2.16 Cold Junction Temperature Parameter Qualification

There is one Cold Junction Temperature sensor on each channel. Each sensor is used for making temperature corrections on its respective channel for the HPOT and HPFT Discharge Temperature sensors. [IR795:6164;1] The value of each Cold Junction Temperature sensor shall be verified to be within the limits specified in Table XVII. [IR795:6164;2] If a Cold Junction Temperature sensor is temporarily disqualified, its last qualified value shall be used for making temperature corrections on its respective channel. [IR795:6164;3] If one Cold Junction Temperature sensor is permanently disqualified, the remaining Cold Junction Temperature sensor value shall be used for making the cold junction temperature corrections on both channels. [IR795:6164;4] If both Cold Junction Temperature sensors are temporarily or permanently disqualified, the last qualified Cold Junction Temperature sensor value that was used for making temperature corrections on each channel shall continue to be used for making the cold junction temperature corrections on each channel.

3.2.3:4.3 Sensor/Channel Disqualification

Temporary disqualification of sensors or channels for particular parameters occurs upon failure of qualification tests, according to the criteria specified in 3.2.3:4.2. Permanent disqualification of sensors or channels for particular parameters for specific functions occurs after a specified number of consecutive qualification failures. Nominally permanent disqualification of a sensor or channel occurs when a qualification test fails for three consecutive major cycles. However, if a qualification test is bypassed or delayed, the three consecutive qualification failures may span many major cycles.

The standby DCU will not perform permanent disqualifications, per 3.2.1:8.5.

The inputs from a sensor or channel temporarily or permanently disqualified for a specific function will not be used for that function, but may be used for scaling (3.2.3:4.1), VDT reporting (3.2.2:2.2), and self-qualification (in the case of temporary disqualification), per 3.2.3:4.2.1. In general, but not in all cases, a sensor or channel disqualified for a specific function is disqualified for all functions.

#### 3.2.3:4.3.1 Temporary Disqualification

[IR796:2042;1] When a sensor or channel is temporarily disqualified, only the surviving sensor or channel, if any, shall be used for the specific function until the temporarily disqualified sensor or channel becomes qualified.

[IR796:3407;1] If all other sensors reporting the same parameter have been temporarily or permanently disqualified, the last qualified sensor data shall be used as the parameter's value for purpose of reporting in the VDT. This value may also be used as a control value, see 3.2.3:4.4.2.

[IR796:2218;3] If all sensors reporting the same parameter on a channel have been temporarily disqualified, that channel shall be temporarily disqualified for that parameter.

#### 3.2.3:4.3.2 Permanent Disqualification

[IR799:3814;1] A sensor shall be permanently disqualified for monitoring of the particular parameter upon failure of any of the relevant qualification tests for a specific function, in each of a specified number of major cycles as follows:

- (a) [IR799:6239;1] If the FASCOS Bypass option is not in effect, permanent disqualification of the Vibration Limit Monitor parameters shall occur after qualification failures in seven (operational data) consecutive major cycles during Start Preparation or three (operational data) consecutive major cycles during Mainstage.
- (b) [IR799:3814;3] For all other parameters listed in 3.2.3:4.2 permanent disqualification shall occur after qualification failures in three consecutive major cycles, unless the test is delayed or bypassed, in which case the three consecutive qualification failures could encompass many major cycles.

[IR799:2218;2] If all sensors for a parameter on a channel are permanently disqualified, that channel shall be permanently disqualified for that parameter. [IR799:3814;4] A channel shall be permanently disqualified for monitoring of a particular parameter for a specific function upon temporary disqualification of the channel for monitoring of that parameter, for a specified number of major cycles as listed above.

[IR800:2218;1] There shall be no further qualification monitoring for specific functions of sensors or channels permanently disqualified for those functions.

#### 3.2.3:4.4 Parameter Computation

Qualified sensor data for sensor parameters will be computed as specified in the following requirements.

3.2.3:4.4.1 Channel Values

[IR821:2218;1] Channel values for sensor parameters shall be obtained each major cycle as described below. Sensors or channels are qualified for a parameter as specified in 3.2.3:4.2.2 and Table XVII.

(a) MCC Pc Sensors

- (1) [IR821:2270;1] The MCC Pc channel value shall be set to the average of the values of the MCC Pc sensors on that channel.

(b) Fuel Flowrate Sensors

- (1) Channel values are not calculated for Fuel Flowrate sensors.

(c) Vibration Sensors

- (1) Vibration sensors V1A, V1B, V2A, V2B provide data on distinct parameters. As such, channel values are computed as specified in (e) below.
- (2) [IR821:2218;2] If both V1CA and V1CB sensors, or V2CA and V2CB sensors are qualified, then the channel value, V1C or V2C, shall be set to the average of V1CA and V1CB or V2CA and V2CB in each case.
- (3) [IR821:2218;3] If only one of V1CA and V1CB, or V2CA and V2CB sensors are qualified, then the channel value, V1C or V2C, shall be set to the value of the qualified sensor in each case.
- (4) [IR821:3605;1] If both V1CA and V1CB sensors, or V2CA and V2CB sensors are disqualified, then the channel value, V1C or V2C, shall be set to the average of V1CA and V1CB or V2CA and V2CB in each case.

(d) HPOT and HPFT Discharge Temperature Sensors

- (1) [IR821:6164;1] The channel value shall be set to the average of the qualified sensor values on that channel; but if all sensors are temporarily or permanently disqualified, the channel value shall be set to the last qualified value.

(e) Single Sensor Parameters

- (1) [IR821:2218;4] Channel values for parameters for which there is only one sensor on the channel shall be identical to the value of the respective sensor.

3.2.3:4.4.2 Control Values

[IR822:1608;1] For each control parameter, a control value shall be obtained according to the following.

- (a) [IR822:5522;1] Except for Fuel Flowrate, if both channels of the control parameter are qualified, then the control value shall be set to the average of the values of the two channels, for that parameter.
- (b) [IR822:5522;2] Except for Fuel Flowrate, if only one channel is qualified for a control parameter, then the control value shall be set to the channel value for the parameter, of the qualified channel.
- (c) [IR822:5522;3] If neither channel of the control parameter is qualified, then the control value shall remain set to the last value determined from qualified channel(s), with the exception of MCC Pc and Fuel Flowrate.
- (d) [IR822:2218;1] For MCC Pc, if both channels are temporarily disqualified, or if one channel is temporarily disqualified and the other channel is permanently disqualified, then the control value shall remain set to the last value determined from qualified channel(s).
- (e) [IR822:5469;1] Between Start + 0.80 sec and Start + 1.48 sec, if both channels are permanently disqualified for MCC Pc, then the control value shall be set equal to 50 psia.
- (f) [IR822:5469;2] For all other times, if both channels are permanently disqualified for MCC Pc, then all MCC Pc sensors within the limits of 1000 and 3500 psia shall be averaged. [IR822:3981;2] This average shall then be used for the control value. [IR822:3981;3] If all the sensors fail this screening test, then the control value shall be set to the Pc Reference value. [IR822:4462;1] A failure shall be reported the first time Pc Reference is reported as the control value during Mainstage.
- (g) [IR822:5800;1] For Fuel Flowrate, the control value shall be set to the average of all qualified sensors which update. [IR822:5522;5] If no Fuel Flowrate sensors are qualified, then the control value shall be set to the last value determined from qualified sensors.

3.2.3:4.4.2 Control Values (Continued)

- (h) [IR822:5864;1] From 40% RPL to Start + 3.5 seconds, qualified LPFP Discharge Pressure and LPFP Discharge Temperature sensor values shall be screened using the Sensor Qualification limits defined for Start + 3.5 seconds (Table XVII). [IR822:5864;2] The screened values determined in this manner shall be used as the qualified values in (a), (b), or (c) above to determine the control values. These control values are used in the fuel density calculation in Table XVI.



### 3.2.3:5 Engine Limit Monitoring

This section describes the requirements for monitoring performance of the engine and its components, and responding to detected malfunctions or failures associated with the SSME.

The functions specified here relate to the Engine Firing Operations. Other tasks associated with Checkout Standby which involve introduction of test functions and signals in a non-operational environment were described under 3.2.3:2.

[IR823] The in-control DCU shall have the capabilities described in this section when an FRT or Flight Configuration is active. The engine state monitoring requirements for the standby DCU are specified in 3.2.1:8. In the following paragraphs, when confirmation of failure to pass the monitoring test criteria is required, the applicable number of repeated tests (strikes) is individually specified. [IR824] Otherwise, the indicated failure response shall be executed on first detection of discrepancy.

#### 3.2.3:5.1 Conditions for Engine Ready

The purpose of Engine Ready monitoring is to determine if the engine can commence ignition. Engine Ready monitoring is performed during the Purge Sequence Four mode, and during the Engine Ready mode with Start Enable not in effect. While in the Purge Sequence Four mode, if the Engine Ready conditions are satisfied and there is no I-response failure in effect, the engine mode will be switched automatically to Engine Ready. While in the Engine Ready mode and Start Enable is not in effect, if the Engine Ready conditions are not satisfied, reversion to Purge Sequence Four will occur per Table X Part H (Purge Sequence Four Rollback). Sensors used to determine Engine Ready are qualified per 3.2.3:4.2.6.

Engine Ready monitoring will be initiated during Purge Sequence Four at the times indicated in Table X, Parts D and H. [IR826:2326;1] During Engine Ready monitoring, the sensor values of the following sensors shall be compared with the Engine Ready limits shown in Table XVIII.

- (a) LPFP Discharge Pressure (dual)
- (b) LPFP Discharge Temperature (dual)
- (c) Preburner Pump Discharge Temperature (dual)
- (d) LPOP Discharge Pressure (dual)

3.2.3:5.1 Conditions for Engine Ready (Continued)

- (e) Emergency Shutdown Pressure (dual)
- (f) Fuel Preburner S/D Purge Pressure (Ch A only)
- (g) Oxidizer Preburner S/D Purge Pressure (Ch B only)
- (h) MOV Hydraulic Temperature (dual)
- (i) MFV Hydraulic Temperature (dual)

[IR827:4254;1] Engine Ready monitoring of an MOV or MFV Hydraulic Temperature sensor shall be bypassed if that sensor has failed the Purge and Ancillary Systems monitor per 3.2.3:6.4 during Start Preparation and the sequence has been continued by a Resume command. In addition, all sensors which have previously failed the Engine Ready condition and have been removed from the list of sensors to be monitored, under (n) below or 3.2.3:1.2.6(b) (2), will also be bypassed.

[IR828:3050;1] While in Purge Sequence Four, the Engine Ready mode shall be entered per 3.2.3:1.2.5 if all monitored Engine Ready sensors have been concurrently within their qualification and Engine Ready limits for a continuous period of 2.0 sec and no I-response is in effect.

[IR830:2683;1] Once in Engine Ready mode with Start Enable not in effect, the applicable sensors shall continue to be monitored to be within their Engine Ready limits.

[IR830:3050;2] If an Engine Ready sensor is outside its Engine Ready limits for a continuous period of 1.0 sec, the Engine Ready condition shall be negated. [IR830:3050;3] Temporary disqualification of the sensor being monitored shall not affect the 1.0 sec period. [IR830:3050;4] If the Engine Ready condition is negated, the following shall occur:

- (j) [IR833:1843;1] That sensor shall be declared as failing the Engine Ready condition.
- (k) [IR836:1826;1] All sensors that failed the Engine Ready condition (FID 12) shall be reported.
- (l) [IR837:1826;1] An I-response failure shall be implemented for each sensor that failed the Engine Ready condition.

3.2.3:5.1 Conditions for Engine Ready (Continued)

- (m) Purge Sequence Four Rollback will be performed per Table X, Part H.
- (n) [IR838:1826;1] All sensors that failed the Engine Ready condition shall be removed from the list of sensors that require Engine Ready monitoring.

3.2.3:5.2 Ignition Confirmation

[IR840:2218;1] Monitoring of MCC Pc at two distinct times, Antiflood Valve (AFV) Position, and HPFP Shaft Speed for Ignition Confirmation shall commence respectively at the times specified in Table XIX and Table XI.

[IR840:2218;2] Monitoring for Ignition Confirmation shall be performed once each major cycle, and shall continue until the parameter passes its ignition confirmation constraints once during each monitoring period or until three failures occur.

[IR840:2218;3] An ignition confirmation parameter shall be considered to pass ignition confirmation constraints if it satisfies the following criteria, as detailed in Table XIX:

(a) MCC Pc Sensors:

- (1) [IR840:2218;4] At least one channel shall be qualified for MCC Pc Monitoring for Ignition Confirmation, per the qualification tests of 3.2.3:4.2.4(a), for each of two distinct monitoring periods.
- (2) [IR840:2218;5] Each channel qualified for MCC Pc monitoring for Ignition Confirmation shall be within Ignition Confirmation Limits at least once during each monitoring period.

(b) HPFP Shaft Speed Sensors:

[IR840:2218;6] At least one HPFP Shaft Speed sensor shall be qualified for Ignition Confirmation monitoring per 3.2.3:4.2.4(b).

3.2.3:5.2 Ignition Confirmation (Continued)

[IR840:2218;7] Each HPFP Shaft Speed sensor qualified for Ignition Confirmation monitoring shall be within Ignition Confirmation limits at least once during the monitoring period.

(c) AFV Position Sensors:

[IR840:4254;1] If both AFV Position sensors have failed Purge and Ancillary System Monitoring in Start Preparation and the sequence has been continued by a Resume command, the AFV Position constraint for ignition confirmation shall be passed.

[IR840:2218;9] Otherwise, at least one AFV Position sensor shall be qualified for Ignition Confirmation monitoring per 3.2.3:4.2.4(c).

[IR840:2218;10] Each AFV Position sensor qualified for Ignition Confirmation monitoring shall be within Ignition Confirmation limits at least once during the monitoring period.

[IR848:2218;1] Ignition shall be confirmed when all ignition confirmation parameters have passed the applicable ignition confirmation constraints.

[IR850:2042;1] If any ignition confirmation parameter does not pass its applicable ignition confirmation constraints at least once in the three major cycles of each monitoring period, the engine shall be reported to have failed ignition, Start Sequence shall be immediately terminated (aborted) and shutdown shall be initiated.

[IR850:1608;1] Upon takeover by DCU B in Start, DCU B shall perform all portions of Ignition Confirmation Monitoring not completed by DCU A.

3.2.3:5.3 Shutdown Limit (Redline) Monitoring

[IR854:5889;1] Shutdown Limit Monitoring shall be initiated at various times in the Engine Start and Mainstage phases and shall continue throughout the Mainstage phase per Table XX. (See Limit Control Enable and Limit Control Inhibit vehicle commands in Table V). The parameters monitored are:

Main Combustion Chamber Pressure  
 HPFT Discharge Temperature  
 HPOT Discharge Temperature  
 HPOP IMSL Purge Pressure  
 HPOT Secondary Seal Cavity Pressure  
 HPFP Coolant Liner Pressure  
 Fuel Preburner Shutdown Purge Pressure  
 Oxidizer Preburner Shutdown Purge Pressure

[IR855:2218;1] Shutdown Limit Monitoring of a sensor or channel shall be performed only if the sensor or channel is qualified per 3.2.3:4.2.3. [IR855:2218;2] The average of the two MCC Pc values on a channel qualified for MCC Pc Shutdown Limit Monitoring shall be used for Shutdown Limit Monitoring. [IR855:2218;3] For all other Shutdown Limit parameters the sensor values shall be used individually. [IR857:6164;1] Each sensor or channel qualified for a Shutdown Limit parameter shall be individually monitored once per major cycle and verified to be within its appropriate limits as specified in Table XX.

[IR857:2218;2] If all sensors or all channels have been disqualified for Shutdown Limit Monitoring of a parameter, Shutdown Limit Monitoring of that parameter shall be discontinued.

3.2.3:5.3.1 Shutdown Limit (Redline) Failure Responses

[IR860:2218;1] When the value of a qualified sensor or channel for a Shutdown Limit Monitor parameter has exceeded its specified limits (see Table XX) for three successive major cycles, it shall be confirmed as having failed its Shutdown Monitor limits. [IR861] The confirmed failure state shall be maintained as long as the value exceeds its specified limits.

[IR862:3828;1] A single successful monitoring test or a temporary disqualification of a sensor or channel shall cancel the confirmed failure state and/or all previous Shutdown Limit Monitor strikes against that sensor or channel.

3.2.3:5.3.1 Shutdown Limit (Redline) Failure Responses  
(Continued)

[IR866:3828;1] A Shutdown Limit Exceeded condition shall be established and maintained (ref 3.2.4:2(e)) as long as:

- (a) All qualified sensors or channels of a parameter are in a confirmed failure state,  
and
- (b) No sensor or channel for that parameter is temporarily disqualified.

[IR874:3828;1] Every time a confirmed failure state is established for a sensor or channel, and/or a Shutdown Limit Exceeded condition is established for a parameter, a failure report and response shall occur.

[IR875:6189;1] When Shutdown Limit Exceeded and Limit Control Enable are concurrently in effect, shutdown shall be initiated and the shutdown failure report and response shall occur for the last qualified sensor or channel for which a confirmed failure state was established. This shutdown will be delayed until Start + 1.50 sec if a failure occurs for either the Fuel or Oxidizer Preburner Shutdown Purge Pressure between Start + 0.80 sec and Start + 1.48 sec.

If the HPOP IMSL Purge Pressure has exceeded the Shutdown Limit criteria, regardless of the Limit Control status, the Backdoor Purge response of 3.2.3:5.5 will be invoked upon entry into Hydraulic Shutdown.

3.2.3:5.4 FASCOS Limit Monitoring

During Mainstage, Flight Accelerometer Safety Cut-Off System (FASCOS) Limit Monitoring of high pressure pump vibration is performed to detect excessive vibration levels that would require the engine to be shut down. (See Limit Control Enable and Limit Control Inhibit vehicle commands in Table V).

[IR877:6239;1] FASCOS Limit Monitoring of a vibration channel shall be performed only if the vibration channel is qualified per 3.2.3:4.2.8, and the FASCOS Bypass option is not in effect. [IR877:3828;2] In each major cycle during the time period specified in Table XX, all qualified vibration channels (3.2.3:4.2.8) shall be compared against the vibration limits specified in Table XX. [IR877:5344;1] An exception is that the comparison shall be suspended on all vibration channels for three major cycles after a recoverable power transient on either DCU channel.

[IR877:3828;3] If at least two vibration channels on a pump are disqualified, FASCOS Limit Monitoring for that pump shall be discontinued.

3.2.3:5.4.1 FASCOS Limit Failure Responses

[IR877:3828;4] When a qualified vibration channel value has exceeded its specified limits (see Table XX) for five (operational data) consecutive major cycles, it shall be confirmed as having failed its FASCOS limits. [IR877:3828;5] This confirmed failure state shall be maintained as long as the channel value exceeds its specified limits.

[IR877:3828;6] A single successful monitoring test or a temporary disqualification on a vibration channel shall cancel the confirmed failure state and/or all previous FASCOS strikes against that channel. [IR877:5344;2] A recoverable power transient on either DCU channel shall cancel the confirmed failure state and/or all previous FASCOS strikes against all the vibration channels.

[IR877:3828;7] A Shutdown Limit Exceeded condition shall be established and maintained (ref 3.2.4:2(e)) as long as either:

(a) All three channels on a pump are in a confirmed failure state.

or

(b) Two channels on a pump are in a confirmed failure state and the third channel is disqualified.

[IR877:3828;8] Every time a confirmed failure state is established for a channel, and/or a Shutdown Limit Exceeded condition is established for a pump, a failure report and response shall occur.

[IR877:3828;9] When Shutdown Limit Exceeded and Limit Control Enable are concurrently in effect, shutdown shall be initiated.

3.2.3:5.5 Backdoor Purge Initiation Monitoring

If sufficient purge pressures are not detected during Hydraulic Shutdown, the Emergency Shutdown solenoid will be deenergized in order to purge the engine via the vent ports of the pressure activated valves of the Pneumatic Control Assembly. The initiation of engine purges in this manner is known as the Backdoor Purge. A Backdoor Purge will be initiated if Hydraulic Shutdown is entered and the HPOP IMSL Purge Pressure has previously exceeded its Limit Shutdown (Redline) limits. A Backdoor Purge will also be initiated if the HPOP IMSL Purge Pressure, Pogo Precharge Pressure, or either Preburner S/D Purge Pressure exceeds the limits shown below during Hydraulic Shutdown. Qualification of these parameters for usage in Backdoor Purge Initiation Monitoring is described in 3.2.3:4.2.9.

[IR879:2218;1] If Hydraulic Shutdown is entered and the HPOP IMSL Purge Pressure Shutdown Limit (Redline), 3.2.3:5.3.1, had been exceeded any time during Start or Mainstage (independent of Limit Control Status) the Backdoor Purge response shall be invoked.

[IR879:1625;2] Each qualified sensor of the following parameters shall be monitored in Hydraulic Shutdown during the times and against the limits given below:

<u>Parameter</u>	<u>Monitoring Times (inclusive) in Hydraulic Shutdown</u>	<u>Lower Limit (inclusive)</u>	<u>Upper Limit (inclusive)</u>
HPOP IMSL Purge Pr	0.0 thru 13.5 sec	170 psia	600 psia
Pogo Precharge Pr	0.12 thru 4.0 sec	600 psia	1500 psia
Fuel/Oxidizer Preburner S/D Purge Pr	2.0 thru 13.5 sec	300 psia	1500 psia

[IR879:4279;1] The Backdoor Purge response shall be invoked for any of the following conditions:

- (a) All qualified HPOP IMSL Purge Pressure sensors have exceeded their above stated limits for three consecutive major cycles and Hydraulic Shutdown was initiated from Start or Mainstage.
- (b) All qualified Pogo Precharge Pressure sensors have exceeded their above stated limits for three consecutive major cycles and Hydraulic Shutdown was initiated from Mainstage.



3.2.3:5.5 Backdoor Purge Initiation Monitoring (Continued)

- (c) All qualified Fuel and Oxidizer Preburner Shutdown Purge Pressure sensors have exceeded their above stated limits for three consecutive major cycles and Hydraulic Shutdown was initiated from Mainstage.
- (d) All sensors for any of the parameters are disqualified and Hydraulic Shutdown was initiated.

[IR879:3074;1] When invoked, the Backdoor Purge response shall deenergize the Emergency Shutdown solenoid immediately, report the failure, and suspend further monitoring of all Backdoor Purge Limits.

### 3.2.3:6 Engine Component Functions

#### 3.2.3:6.1 Actuator Data Processing

[IR880] The engine propellant valves are controlled via actuators which shall be commanded and monitored by the in-control DCU. The actuator commands are scaled and loaded into Output Electronics (OE) storage registers. The OE converts the scaled digital commands into analog parameters that are used to move the actuators. Actuator position monitoring is comprised of Servoactuator Error Indication Interrupt (SEII) monitoring, RVDT Comparison Test, and Channel B RVDT Test in Start Preparation.

For a functional description of the electronics involved in commanding the actuators, see Figure 7.

##### 3.2.3:6.1.1 Actuator Scaling

In order to command actuators via the Output Electronics and monitor actuators via the Input Electronics, data to and from actuators must be scaled.

- (a) [IR880:2982;1] The nominal scaling coefficients used to convert actuator commands (%) to the 12 bit Latching Digital to Analog (LDA) input shall be as specified in Table XXIX. These scaling coefficients are independent constants for the individual actuator channels. Every actuator will have its own unique set of scaling coefficients.
- (b) [IR880:4315;1] The scaling coefficients used to convert the D/A output voltages to their corresponding LDA inputs shall be as specified in Table XXVIII Part F.
- (c) The nominal scaling coefficients used to convert the RVDT output of an actuator to an actuator position are shown in Table XXVIII Part E. These coefficients are independent constants for individual actuator channels. Every actuator will have its own unique set of scaling coefficients.

3.2.3:6.1.2 Actuator Command Processing

[IR881] Command timing and repetition shall be compatible with the control loop computational requirements as stated in 3.2.3:1.4 and nominal major cycle processing per 3.2.1:2.1.

[IR883:2092;1] If RVDT/LVDT excitation for the controlling actuator channel is qualified, the D/As shall be updated and monitored as specified below:

- (a) [IR884:1386;1] Each D/A, whose current contents differs from its desired updated value, shall be updated as part of the normal sequencing, per 3.2.1:2.1, regardless of engine phase/mode.

To update a D/A, the 12 MSBs of the scaled actuator command are concatenated with the appropriate 4 LSB code, per Table XXXIII, and stored in the OE Storage Register. [IR886:1386;1] The D/A command word shall be loaded into the storage register and verified per 3.2.3:3.1.7, OE Storage Registers Self-Test. [IR887] After the contents of the OE storage register have been successfully verified, the command shall be transferred to the D/A by issuing the Transfer OE Storage Register I/O instruction, per Table XXXVIII.

- (b) The OE Digital to Analog converters Self-Test (3.2.3:3.3.5) will be performed.

3.2.3:6.1.3 Servoactuator Error Indication Interrupt Monitoring

A hardware monitor compares the output of each RVDT channel with that of an Actuator Model driven by the respective D/A command. In OE A, when the difference at the comparator is greater than +/-6% of full-opening travel of a nominal OPOV, the actuator channel is indicated as out-of-limits. In OE B, the tolerance is +/-10% of full-opening travel of a nominal OPOV. These out-of-limit conditions are indicated by individual bits in an input word that represent the status of the respective actuator channels. When these limits are exceeded, the corresponding servoactuator error indication is activated. This will trigger a Servoactuator Error Indication Interrupt (SEII) within the DCU if the interrupt level exceeds the CPU interrupt level and the servoactuator error indication is enabled in the CIE.

### 3.2.3:6.1.3 Servoactuator Error Indication Interrupt Monitoring (Continued)

[IR893:2625;1] Monitoring of these servoactuator error indications shall be continuous except for suspension of SEII monitoring as specified within this section. [IR894:1386;1] Only the in-control servoactuator channel shall be monitored by enabling its servoactuator error indications in the CIE and by enabling the SEII.

All servoactuator channels are cross-connected to each DCU; i.e., any one of the channel A or channel B out-of-limits conditions generates the SEII to both DCU A and DCU B. [IR896] Therefore, to preclude the standby DCU from processing responses from I/O hardware it is not controlling, the standby DCU shall disable all servoactuator error indications in the standby CIE, using the Load CIE Interrupt Mask Register Two I/O instruction defined in Table XXXVIII with the bit assignments of Table XXXIX.

SEIIs in the actuator channel which is in control will be monitored unless suspended per the criteria given below. SEII monitoring is suspended when the servoactuator error indications of the in-control actuator channel are disabled by conditions within this paragraph, e.g., disqualification, power transient or pneumatic shutdown.

[IR896:2625;1] All suspensions shall start with the initiating event (e.g., failure detection) and shall continue as specified below. [IR896:2625;2] All timed suspensions shall be measured in the number of complete major cycles starting with the first major cycle following the initiating event. [IR896:2625;3] When the SEII monitor is to be resumed, the SEII shall be cleared before the appropriate servoactuator error indications are enabled in the CIE. [IR896:2625;4] SEII monitoring shall be suspended as follows:

#### Initiation and test:

- (a) [IR896:2625;5] Shall be suspended during entry from PROM processing (3.2.1:1.3).
- (b) [IR896:2625;6] Shall be suspended during Major Cycle Initiation (3.2.1:2.2).
- (c) [IR896:2625;7] Shall be suspended during Major Cycle Restart (3.2.1:2.3).
- (d) [IR896:2625;8] Shall be suspended during the OE Servoactuator Model/Monitor Self-Test per 3.2.3:3.2.4.

### 3.2.3:6.1.3 Servoactuator Error Indication Interrupt Monitoring (Continued)

#### Failure responses:

- (e) [IR896:2625;9] Shall be suspended on a disqualified servoactuator channel (3.2.1:6.4).
- (f) [IR896:2625;10] Shall be suspended for three major cycles following servoactuator channel switchover due to a single channel A SEII for the servoactuator that failed, and one major cycle for those that did not fail (3.2.3:6.1.4). This allows the actuator position to return to within SEII monitoring limits in case of a ramped command; however, the propellant valve may travel at its maximum slew rate during this time.
- (g) [IR896:5193;1] Shall be suspended during power loss in either channel and for three major cycles subsequent to power recovery.
- (h) [IR896:5193;2] Shall be suspended for one major cycle after a DCU B takeover (3.2.1:9.1.2).
- (i) [IR896:2625;13] Shall be suspended for one major cycle after a switchover to servoactuator Channel B resulting from any of the following:
  - (1) The disqualification of OE A (3.2.1:6.3).
  - (2) A RVDT Comparison Test failure followed by a Blueline Limit being exceeded (3.2.3:6.1.4).
  - (3) A Servoactuator Model/Monitor Failure (3.2.3:3.2.4).
  - (4) D to A Converter Failure (3.2.3:3.3.5).
- (j) [IR896:2625;14] Shall be suspended whenever RVDT/LVDT Excitation is deactivated or temporarily disqualified (3.2.3:3.3.4).
- (k) [IR896:2979;1] Shall be suspended upon disqualification of an IE channel, OE channel, servoactuator channel, or cross-channel DCU/IE/OE, until the first major cycle subsequent to Major Cycle Restart, unless superseded by any of the above requirements (e) through (j).

3.2.3:6.1.3 Servoactuator Error Indication Interrupt Monitoring (Continued)

Engine state:

- (l) [IR896:2625;15] Shall be suspended during Hydraulic Lockup (3.2.3:1.7.2).
- (m) [IR896:4279;1] Shall be suspended during portions of the Pneumatic Shutdown Sequence, Table XIV.
- (n) [IR896:2850;1] Shall be suspended for 9.50 +/- 0.04 seconds upon entry into Checkout Standby from a different phase/mode or by a Controller Reset command (3.2.3:1.1.2).
- (o) [IR896:2625;18] Shall be suspended during Controller Checkout (3.2.3:2.3.5).
- (p) [IR896:4043;1] Shall be suspended during portions of Pneumatic Checkout (Emergency Shutdown) as specified in Table XXV.
- (q) [IR896:2625;20] Shall be suspended during Actuator Checkout (Table XXIV).
- (r) [IR896:5376;1] When the Close Emergency Shutdown Valve command is accepted, the SEII for CCV shall be suspended. SEII monitoring for the CCV will be restored upon entry into Checkout Standby, per 3.2.3:1.1.2. This will not affect monitoring of the other four servoactuators.
- (s) [IR896:3300;1] Shall be suspended when the configuration is FRT-2 (3.2.3:2.4.1:1.2).
- (t) [IR896:2625;23] Shall be suspended during the pneumatic closure period of the Terminate Sequence mode of Post Shutdown (Table XV, Part A).
- (u) [IR896:6152;1] Shall be suspended during Actuator Pre-operational Conditioning Cycle (3.2.3:2.3.8).

RVDT Comparison Test (3.2.3:6.1.4), Channel B RVDT Monitoring in Start Preparation (3.2.3:6.1.5), and OE Servoactuator Model/Monitor Self-Test (3.2.3:3.2.4) will not be performed when SEII monitoring is suspended.

3.2.3:6.1.3:1 Responses to Unscheduled SEII

[IR906:4194;1] Receipt of an SEII shall require validation and response per the following and as defined in Table I for the specified FIDs. The processing described herein is applicable only when an unscheduled interrupt occurs, i.e., it is not applicable either during the OE Servoactuator Model/Monitor Self-Test (3.2.3:3.2.4) or during Actuator Checkout when scheduled interrupts occur either by use of the hardware interrupt self-test function or by other means which purposely force the interrupts.

- (a) [IR906:1386;1] When the SEII is received, all the servoactuator error indication pending bits (in input word seven) for the servoactuator error indications that have been enabled in the CIE shall be stored in RAM as they exist upon entry into the interrupt response sequence.
- (b) If monitoring has been suspended by disabling all servoactuator error indications in the CIE, the response will be in accordance with the Interrupt Decoder Self-Test of 3.2.3:3.1.5.
- (c) If monitoring is in effect but there are no corresponding pending bits for the servoactuator error indications that have been enabled, the response will be in accordance with the Interrupt Decoder Self-Test of 3.2.3:3.1.5.
- (d) [IR906:1386;2] If more than one servoactuator error indication is pending for the in-control servoactuator channel, the respective OE channel shall be disqualified per 3.2.1:6.3. This accommodates common failures.

3.2.3:6.1.3:1 Responses to Unscheduled SEII (Continued)

- (e) [IR906:1386;3] If only one servoactuator error indication is pending for the in-control servoactuator channel, a delay of 200 to 300 usec shall be performed prior to issuing a Clear SEII I/O instruction which clears all the servoactuator error indication pending bits. [IR906:1386;4] All of the in-control servoactuator channel servoactuator error indication pending bits shall be rechecked.

After rechecking:

- (1) [IR906:1386;5] If only the original servoactuator error indication is pending, the following shall apply:
- (i) [IR906:1386;6] Any IE input sequence currently in progress shall be terminated.
  - (ii) [IR906:1386;7] The IE input sequence shall be initiated to input the servovalve current monitor value for both channels of the servoactuator that caused the SEII.
  - (iii) The servovalve current monitor value will be the Failure Parameter value issued with the failure report.
  - (iv) [IR906:1386;8] If control has been via Channel A servoactuators, and Channel B servoactuators are qualified, the Channel B servoactuator error indications shall be enabled in the CIE. [IR906:1386;9] The Channel B servoactuator error indication pending bits shall be examined.
    - a. [IR906:1386;10] If Channel B of the servoactuator indicated above as failed has a pending servoactuator error indication, and no other Channel B servoactuator has a pending servoactuator error indication, both Channel A and B servoactuators shall be disqualified per 3.2.1:6.4. This guards against critical cases of switching to a failed servoactuator channel while SEII monitoring is suspended.



3.2.3:6.1.3:1 Response to Unscheduled SEII (Continued)

- b. [IR906:3520;1] Else, if there is a single servoactuator error indication on Channel B that is different from Channel A, or multiple Channel B servoactuator error indications, Channel A servoactuators shall be disqualified per 3.2.1:6.4.
  - c. [IR906:3520;2] Else, if there was a prior RVDT miscompare for any servoactuator, Channel A servoactuators shall be disqualified per 3.2.1:6.4. The failure will be reported as a Channel A Actuator SEII with a prior RVDT Miscompare.
  - d. [IR906:3520;3] Else, Channel A servoactuators shall be disqualified per 3.2.1:6.4.
- (v) [IR906:1386;12] Else, if control has been via Channel A servoactuators, and Channel B servoactuators are disqualified, Channel A servoactuators shall be disqualified per 3.2.1:6.4.
- (vi) [IR906:1386;13] Else, since control has been via Channel B servoactuators, Channel B servoactuators shall be disqualified per 3.2.1:6.4.
- (2) [IR906:1386;14] Else, if any in-control servoactuator channel servoactuator error indication is pending which differs from the original, the in-control OE channel shall be disqualified per 3.2.1:6.3.
- (3) [IR906:1386;15] Else, since no servoactuator error indications are pending, a Major Cycle Restart shall be performed.

3.2.3:6.1.4 RVDT Comparison Test

The actuator monitoring tests of this and the next paragraph (3.2.3:6.1.5) detect servoactuator driver failures (on a single strike basis) not discernible by servoactuator error indications. Qualification of parameters for usage in RVDT Comparison Monitoring is described in 3.2.3:4.2.10.

[IR907:2625;1] If both servoactuator channels are qualified, all five propellant valves shall be checked by the in-control DCU during Start Preparation, Start, Mainstage, and Hydraulic Shutdown to verify that the Channel A and Channel B RVDT positions agree within a tolerance of 3%. [IR908:4184;1] The RVDT comparison test shall be performed after the OE Digital to Analog Converters Self-Test (3.2.3:3.3.5) within the major cycle. This is to prevent an entry into Hydraulic Lockup because of a disqualified IE causing an RVDT miscompare followed immediately by a D/A converter failure.

[IR908:2625;1] The RVDT comparison test shall be suspended during periods when SEII monitoring is suspended (3.2.3:6.1.3) or, the OE RVDT/LVDT Excitation Power Supply Self-Test (3.2.3:3.3.4) is either suspended or a failure has occurred within the self-test. [IR909:2625;1] The RVDT Comparison Test shall cease after the RVDT Comparison Test has failed.

[IR909:1608;1] This RVDT comparison test shall also be suspended during the time that an I-response, due to RVDT miscompare, is in effect. [IR909:2625;2] The comparison test shall be reinstated when the I-response is no longer in effect. [IR909:5451;1] All indications of a prior RVDT miscompare shall be reset to indicate that no RVDT miscompare has occurred following acceptance of a Resume command in the Start Preparation phase when all Inhibit Responses are cleared.

Subsequent to a failure of the RVDT comparison test the following will pertain:

3.2.3:6.1.4 RVDT Comparison Test (Continued)

- (a) [IR911:2266;1] If both servoactuator channels are qualified and the Blueline Limits (Table XX) are active, HPOT and HPFT Discharge Temperature sensor values shall be verified against the Blueline Zones. A Blueline Zone is defined as the range of sensor values within the Blueline Limit and the closest corresponding Qualification Limit (Table XVII). [IR912:1608;1] If all qualified HPOT or HPFT Discharge Temperature sensors are within the Blueline Zones, Channel A servoactuators shall be disqualified.
- (b) If the engine phase is Start, Pneumatic Shutdown will be declared for a Channel A servoactuator disqualification unless the disqualification was due to Blueline Limit Monitoring.
- (c) If the engine phase is Mainstage, Hydraulic Lockup will be declared for a Channel A servoactuator disqualification unless the disqualification was due to Blueline Limit Monitoring.
- (d) [IR912:5451;1] If an RVDT miscompare has occurred, Pneumatic Shutdown shall be performed when Shutdown is requested.

3.2.3:6.1.5 Channel B RVDT Monitoring in Start Preparation

[IR913:1608;1] If the Channel A servoactuators are disqualified and the engine phase is Start Preparation, the Channel B RVDT positions of all propellant valves shall be verified to be at least -3% open. [IR914:3764;1] This Channel B -3% test shall be suspended during periods when SEII monitoring is suspended (3.2.3:6.1.3), or the OE RVDT/LVDT Excitation Power Supply Self-Test (3.2.3:3.3.4) is either suspended or a failure has occurred within the self-test. [IR914:3764;2] The Channel B -3% test shall cease after the Channel B -3% test has failed.

[IR915:1608;1] If the Channel B -3% test fails for a propellant valve, Channel B servoactuators shall be disqualified.

3.2.3:6.1.6 Actuator Exercise Sequence

[IR945:5535;1] The Actuator Exercise Sequence shall be performed if the following conditions are met:

- (a) Both servoactuator channels are qualified.
- (b) IE B is not permanently disqualified.
- (c) There is no I-Response in effect.
- (d) The Hydraulic System pressure is greater than or equal to 300 psia and less than or equal to 600 psia.

3.2.3:6.1.6 Actuator Exercise Sequence (Continued)

[IR945:1625;2] If any of the above stated conditions fail to be met during the Actuator Exercise Sequence, the sequence shall be exited.

[IR945:6152;1] The Actuator Exercise Sequence, shall be performed on each servoactuator in turn (MFV, MOV, CCV, FPOV, OPOV) until each servoactuator has completed this exercise 120 times. [IR945:2275;1] The Actuator Exercise sequence shall be performed during the Fuel System Purge of Purge Sequence 3.

[IR945:6152;2] The 300 msec sequence shall be as follows:

- (a) Delay 20 msec.
- (b) Energize the fail-operational servoswitch of the selected servoactuator.
- (c) Delay 20 msec.
- (d) Command Channel A of the servoactuator to +3%.
- (e) Delay 40 msec.
- (f) Command Channel A of the servoactuator to 0%.
- (g) Delay 60 msec.
- (h) Deenergize the fail-operational servoswitch.
- (i) Delay 20 msec.
- (j) Command Channel B of the servoactuator to +3%.
- (k) Delay 40 msec.
- (l) Command Channel B of the servoactuator to 0%.
- (m) Delay 60 msec.
- (n) Energize both fail-safe servoswitches.
- (o) Delay 20 msec.
- (p) Deenergize both fail-safe servoswitches.
- (q) Delay 20 msec.

The Actuator Exercise Sequence is diagrammed for information only in Figure 11A.

[IR945:6152;3] Upon completion or termination of this sequence, the fail-operational servoswtiches shall be set to the state dictated by the hardware qualification status.

3.2.3:6.1.7 Actuator Settling Check

An actuator settling check of the MFV, MOV, FPOV, and OPOV will be performed by comparing average actuator positions in Purge Sequence 3 to those in Purge Sequence 4. [IR945:4555;1] Actuator channels shall be qualified for use in the Actuator Settling Check per 3.2.3:4.2.15. Requirements for this check are as follows:

- (a) [IR945:5795;1] During Purge Sequence 3, position averages for all channels of the MFV, MOV, FPOV, and OPOV shall be calculated. [IR945:4555;2] Each set of averages shall be calculated using 128 qualified position samples; and these averages shall be updated for each subsequent 128 qualified samples. [IR945:3070;3] The last set of averages determined in Purge Sequence 3 shall be used for comparison in (d) below.
- (b) [IR945:3070;4] A separate set of position averages shall be continually calculated during Purge Sequence 4 (starting as specified in Table X, Part D). [IR945:4555;3] Each set of averages shall be calculated using 128 qualified position samples; and these averages shall be updated for each subsequent 128 qualified samples. [IR945:3070;6] Updating of averages shall continue until the Actuator Settling Check terminates.
- (c) [IR945:3070;7] Sequencing out of Purge Sequence 4/Engine Ready modes or a successful check shall terminate the Actuator Settling Check.
- (d) [IR945:3070;8] Upon determining each set of Purge Sequence 4 position averages, a comparison shall be made. [IR945:3070;9] For all actuators, if at least one Purge Sequence 4 channel average is less than its respective Purge Sequence 3 channel average by at least 0.1 percent of full open, the Actuator Settling Check shall have passed.
- (e) [IR945:3070;10] If (d) is performed three times and none were successful, the Actuator Settling Check shall be terminated and a failure reported. [IR945:5795;2] If more than one actuator fails, the failure report shall only indicate the first failing actuator. The actuators will be tested in the following order: MFV, MOV, FPOV, and OPOV.
- (f) [IR945:3070;11] The Actuator Settling Check shall be performed every time the engine is commanded into Purge Sequence 4 with no previous failure of the Actuator Settling Check.

### 3.2.3:6.2 Igniter Data Processing

[IR946:1386;1] Both igniter channels shall be commanded on or off in immediate succession when the function is commanded.  
[IR947:3874;1] The three pairs of igniters shall be commanded on, then off, during the Start phase as specified in Table XI.  
[IR948] They shall be commanded off for all other phases, except as required for the Igniter Checkout Test, per 3.2.3:2.3.2.

Igniters are controlled in two sets, one in Channel A and one in Channel B. Each set is operated via one OE On/Off Register command, Energize Igniters A/B per Table XXXI. The igniters will be monitored by means of the Engine/Controller On/Off Devices Self-Test of 3.2.3:3.2.3.

### 3.2.3:6.3 Servoswitch and Solenoid Data Processing

The fail-safe servoswitches, fail-operational servoswitches and the pneumatic solenoids are all controlled via bits within the OE On/Off Registers as defined in Table XXXI.

[IR954:1386;1] The fail-safe valves are controlled by pairs of servoswitches which shall be commanded on or off in immediate succession when the function is commanded. [IR955:2275;1] These valves shall normally be activated and deactivated per the mission phase requirements as defined in Tables X, XIII, and XV. [IR956] They shall also be deactivated when in Checkout or Post Shutdown Standby as well as when in Pneumatic Shutdown or Hydraulic Lockup mode. In addition, the fail-safe servoswitches will be energized or deenergized according to the state of OE RVDT/LVDT excitation (3.2.3:3.3.4).

Each fail-operational valve is controlled by an individual servoswitch. A fail-operational valve will be activated as part of the failure responses, whenever Channel B of the respective actuator is to be used, i.e., Channel A disqualified and Channel B operational, and the corresponding fail-safe valve is activated. See 3.2.1:6.4. However, it is permissible to temporarily activate fail-operational valves for up to one major cycle without the corresponding fail-safe valves being activated.

The fail-operational servoswitches will be deenergized for the following conditions:

- (a) Controller Reset Command
- (b) Actuator Checkout
- (c) Controller Checkout
- (d) Actuator Exercise Sequence

### 3.2.3:6.3 Servoswitch and Solenoid Data Processing (Continued)

[IR959] When the fail-safe and fail-operational valves of an actuator are to be concurrently activated, i.e., both commands to be changed from off to on, the fail-operational valve command shall be issued no later than 1 msec following the issuance of the fail-safe valve command.

The pneumatic valves are individually controlled by two solenoids. [IR960] They shall be commanded on or off in immediate succession when the function is commanded. [IR961:2275;1] The valves shall normally be activated and deactivated as defined in the mission phase sequences of Tables X, XI, XIII, and XV. [IR962] They shall also be deactivated when the mission phase/mode is Checkout Standby, or Pneumatic Shutdown. [IR963] These valves, except for the Bleed Valve Control Valve, shall also be deactivated when the mission phase/mode is Post Shutdown Standby. See Post Shutdown phase (3.2.3:1.6) for details of the Bleed Valve Control Valve activation/deactivation.

Activation of a pneumatic solenoid requires first energizing it at high current level for 50 to 200 msec then maintaining the activated state at a lower current (Hold) level. It takes approximately 30 msec for the solenoids to pull in. The current level common to all solenoids in an OE is controlled via the Pull-In/Hold bits. [IR964:5140;1] When a pneumatic solenoid is commanded from Off to On, or is recommanded On upon recovery from a power transient, the solenoid drive level in that OE shall be commanded to the Pull-In level for three major cycles. [IR964:2001;2] After the last pneumatic solenoid to be commanded On has completed three major cycles at the Pull-In level, the solenoid drive level shall be commanded to the Hold level.

The servoswitches and solenoids will be monitored by the Engine/Controller On/Off Devices Self-Test of 3.2.3:3.2.3. [IR967:2307;1] Monitoring shall be suspended for an individual servoswitch or solenoid following any change in its commanded state, to accommodate the response time defined in paragraph 3.2.3:3.2.3.

3.2.3:6.4 Purge and Ancillary Systems Monitoring

[IR973:2307;1] The parameters listed below shall be monitored by the in-control DCU at the times given in Table XXI.

The parameters monitored are:

- . Emergency Shutdown Pressure
- . Fuel Bleed Valve Position
- . Oxidizer Bleed Valve Position
- . Pogo Recirculation Isolation Valve (RIV) Position
- . Antiflood Valve Position
- . Fuel Purge Pressure
- . HPOP IMSL Purge Pressure
- . Pogo Precharge Pressure
- . MOV Hydraulic Temperature
- . MFV Hydraulic Temperature

[IR976:6156;1] Each sensor value qualified per 3.2.3:4.2.11 shall be individually monitored once per major cycle and verified to be within its respective limits as specified in Table XXI.

[IR979:2218;1] If a sensor has been determined as out of limits for three consecutive major cycles, it shall be indicated as failed. The failure indication will be maintained until acceptance of a Controller Reset command.

[IR980:2307;1] When the commanded state of a solenoid is changed for the purpose of Engine Operations, then monitoring of the associated parameter shall be delayed per Table XXI. [IR980:4700;1] Monitoring shall be delayed one major cycle for all parameters following Major Cycle Restart. [IR980:4700;2] However, if the Major Cycle Restart was due to a recoverable power transient on either channel, the Bleed Valves, Pogo RIV, and Antiflood Valve shall be delayed two major cycles. This is done to accommodate transitory changes in the commanded states due to power loss/recovery or DCU B takeover.



3.2.3:6.4 Purge and Ancillary System Monitoring  
(Continued)

A Purge and Ancillary failure of an MOV or MFV Hydraulic Temperature sensor during Start Preparation will cause Engine Ready monitoring (3.2.3:5.1) of that sensor to be bypassed (if the sequence has been continued by a Resume command). A Purge and Ancillary failure of both AFV Position sensors during Start Preparation will cause Ignition Confirmation monitoring (3.2.3:5.2) of that parameter to be bypassed (if the sequence has been continued by a Resume command).

Purge and Ancillary monitoring will be suspended upon acceptance of a Start Enable command or when Start Enable is terminated per 3.2.3:1.2.6 and Table X, Parts F and G.

3.2.3:6.5 Pogo GOX Flow Check

This test will be bypassed in FRT per 3.2.3:2.4.1:1.1(e). [IR983:2218;1] Monitoring of the two Pogo Precharge Pressure sensors for the Pogo GOX Flow Check shall commence at the time specified in Table XIX.

[IR983:2218;2] Once initiated, monitoring for the Pogo GOX Flow Check shall be performed once each major cycle, and shall continue until each sensor passes the Pogo GOX Flow Check once or until three failures occur.

[IR983:2218;3] A Pogo Precharge Pressure sensor shall be considered to have passed the Pogo GOX Flow Check if it satisfies the criteria below, as detailed in Table XIX:

- (a) The Pogo Precharge Pressure sensor will be qualified for the GOX Flow check, per 3.2.3:4.2.7.
- (b) [IR983:2218;4] Each Pogo Precharge Pressure sensor qualified for the Pogo GOX Flow Check shall be within Pogo GOX Flow Check limits at least once during the monitoring period.

3.2.3:6.6 GN2/He Purge Monitor

[IR984:3981;1] Each qualified HPOP IMSL Purge Pressure sensor shall be monitored during the time and against the limit given below:

<u>Sensors</u>	<u>Monitoring Period</u>	<u>Limit</u>
A, B	Purge Sequence 3 to Start Enable	100 psia

[IR984:3981;2] If a qualified sensor is below this limit for ten consecutive major cycles, a failure shall be reported.

3.2.3:6.7 MCC LOX Dome Temperature Monitor

[IR985:3981;1] The MCC LOX Dome Temperature sensor shall be monitored during the time and against the limit given below:

<u>Sensors</u>	<u>Monitoring Period</u>	<u>Limit</u>
B	Purge Sequence 3 to Start Enable	400 R

[IR985:3981;2] If the sensor is qualified and is below this limit for three consecutive major cycles, a failure shall be reported.

3.2.3:6.8 Preburner Pump Discharge Temperature Sensor Integrity Monitor

[IR985:6244;1] Each qualified Preburner Pump Discharge Temperature sensor shall be monitored during the time and against the limit given below:

<u>Sensors</u>	<u>Monitoring Period</u>	<u>Limit</u>
A, B	Purge Sequence 4 through Mainstage	230 R

[IR985:5345;1] If all qualified sensors are greater than this limit for the same three consecutive major cycles, a failure shall be reported.

### 3.2.3:7 Summary of Engine Control

This section summarizes the requirements to be satisfied in conditioning commands to engine devices. It repeats requirements for information only, all requirements described here have been previously specified in 3.2.3:1.

#### 3.2.3:7.1 Propellant Valve Control Summary

The Checkout phase is the phase to which the Operational Program is initialized to begin active control, monitoring, or checkout of the SSME. During this phase all propellant valves will be kept closed, except when moved as part of a checkout sequence.

During the Start Preparation phase all propellant valves are kept closed except for the CCV which is opened in Purge Sequence 4 as described in Table X Part D.

The Start phase covers the operations for starting of engine firing. It begins with scheduled open-loop operation of propellant valves, then closes the control loops and achieves smooth transition to controlled MCC Pc and mixture-ratio operation of the engine. The Start phase will be initiated upon acceptance of a Start command. The operations and functions applicable to this phase are described in Table XI. Start phase control loop functions are described in Figures 8, 9 and 10.

Mainstage phase is automatically entered upon successful completion of the Start phase described in 3.2.3:1.3. During Mainstage phase, the propellant valves are commanded to provide closed-loop control of the engine MCC Pc and propellant mixture ratio. The control functions will be as described in Figures 8, 9, and 10, based on a major cycle of 20 msec, which results in an update rate of 50 hz. The computational lag will be normally maintained within the limits indicated in 3.2.3:1.4.1.

In performing the Mainstage control function computations, the Tustin method will be used to implement the transfer functions into sampled-data control equations, per 6.3. The CCV is controlled in an open loop manner as a function of Pc Reference using the control laws shown in Figure 10. The MFV and MOV are maintained at 100% open throughout Mainstage.

3.2.3:7.1 Propellant Valve Control Summary (Continued)

In the Shutdown phase engine thrust is reduced and all valves are driven to effect full engine shutdown. Normal shutdown will begin with closed loop control of propellant valves and will complete shutdown via scheduled open loop control of propellant valves per Table XIII, for all cases except when fail-safe Pneumatic Shutdown is specified. Table XIV is executed in fail-safe Pneumatic Shutdown. The design will ensure that the proper engine control and valve sequencing functions and commands are executed during the first major cycle of the Shutdown phase regardless of prior existing phase and mode.

Upon acceptance of a Shutdown Command during a Hydraulic Lockup mode, a Pneumatic Shutdown will be initiated. The Shutdown phase will also be initiated automatically as a result of SSME or controller assembly monitoring. Conditions and sequencing for these cases are described in 3.2.3:5 and 3.2.1.

The Post Shutdown phase represents the state to which the SSME and Controller go at completion of engine firing. The Standby mode of this phase is entered automatically as shown in Figure 6. In the Standby mode of this phase, output devices are maintained as defined in 3.2.3:1.6. The configuration is the same as exists at normal completion of the modes leading to Standby.

Acceptance of a Terminate Sequence Command, or a T-Response will initiate the Terminate Sequence Mode of Post Shutdown phase. Applicable operations and functions are described in Table XV, Part A. Acceptance of an Oxidizer Dump Command will initiate the Oxidizer Dump Mode of the Post Shutdown Phase. At most one main propellant valve will be open at any time in this mode. The sequence and timing for this mode are defined in Table XV, Part B. This mode is ended by a Terminate Sequence Command.

### 3.2.3:7.2 MCC Pc Control Summary

The Start phase begins scheduled open loop operation of propellant valves, then closes the loop and achieves smooth transition to controlled MCC Pc operation of the engine. Applicable operations and functions are described in Table XI. During Mainstage phase, the propellant valves are commanded to provide closed-loop control of MCC Pc in response to MCC Pc commands.

During closed loop control, measured engine MCC Pc will be driven to the values attained by Pc Reference as shown in Figure 8. Pc Reference is equal to the Main Combustion Chamber Pressure Level command under rate limited conditions.

Should both channels of MCC Pc sensors fail, Electrical Lockup or Hydraulic Shutdown will be entered.

In the Shutdown phase engine thrust is reduced and all propellant valves are driven to effect engine shutdown.

#### 3.2.3:7.2.1 Thrust Limiting Summary

After the OPOV/FPOV command is computed, the command is compared to the command limit. If the command exceeds the command limit, the command will be set to the command limit. Control Loop calculations will continue normally while the command is being limited.

While in Mainstage, Thrust Limiting mode will be entered from Normal Control or Fixed Density mode when the OPOV command is limited for 3 consecutive major cycles. Recovery back to Normal Control or Fixed Density mode will occur when the OPOV command is not limited for 3 consecutive major cycles. If there is no recovery, exit from this mode will be caused by a failure or shutdown command. Thus, exit from this mode may be to Electrical Lockup mode, or Hydraulic Lockup mode, or to Shutdown phase.

### 3.2.3:7.3 Mixture Ratio Control Summary

Mixture ratio is computed as the ratio of oxygen to hydrogen weight flowrates. The applicable equations are shown in Table XVI. The valve controlling the mixture ratio is the FPOV.

The Mixture Ratio reference is 6.011. The Start phase begins scheduled open loop operation of propellant valves, then closes the loop and achieves smooth transition to controlled mixture ratio operation of the engine.

The Start phase will be initiated upon acceptance of a Start command. Applicable operations and functions are described in Table XI. During Mainstage phase, the FPOV is commanded to provide closed-loop control of the propellant mixture ratio. Control functions are described in Figures 9 and 10.

#### 3.2.3:7.3.1 Fixed Density Mode Summary

Fixed Density mode is entered as a result of failure or disqualification of both channels of LPFP Discharge Pressure or LPFP Discharge Temperature during Start or Mainstage. Computations of propellant density values will be suspended. A fixed fuel density value will then be used during all processing. See Table XVI, Part A(3) for details.

### 3.2.4 Failure Reporting and Responses

Failure reporting serves a dual purpose, warning of the loss of a real-time engine control function, providing sufficiently detailed data for post-mission analysis and fault isolation, and detailed information on specific DCU failures. For the latter purpose, reports of confirmed failures are entered in failure lists in the VDT to accommodate multiple failures within a VDT transmission interval.

Responses are designed to provide effective utilization of the engine/controller redundancy capabilities and concurrently ensure fail-safe outcomes.

[IR987:6273;1] Failure responses and failure reports shall be per Table I and Table II.

Table I has the various failures grouped by functions involved as follows:

<u>Failure ID</u> <u>(Octal)</u>	<u>Failure Description</u>
1/2	DCU A/B disqualified
3/4	IE A/B disqualified
5/6	OE A/B disqualified
7/10	OE A/B non-disqualifying
111	Sensor First Channel Disqualification
11	Sensor Second Channel Disqualification
12	Engine Ready Parameter failures
113	Shutdown Limit Monitor
13	Shutdown Limit and Ignition Confirmation Monitors
14	Purge and Ancillary Monitoring
15	Actuator Failures
116	FASCOS First Channel Disqualification
16	FASCOS Second Channel Disqualification
117	FASCOS Shutdown Limit Monitor
17	FASCOS Shutdown Limit Exceeded

3.2.4 Failure Reporting and Response (Continued)

<u>Failure ID</u> <u>(Octal)</u>	<u>Failure Description</u>
20	Miscellaneous Reports
21	Propellant Drop Failures
22	Igniter Checkout
23	PSE Logic/Redundancy Tests Support
34	Hydraulic Conditioning
135	Non-Tested Actuator Opens, Actuator Checkout Ch A
35	Actuator Checkout Ch A
136	Non-Tested Actuator Opens, Actuator Checkout Ch B
36	Actuator Checkout Ch B
37	Power Recovery
41	Single Command Channel Shutdown
42	Command Voting Failures
43/44	Sensor Checkout Ch A/B
45/46	Pneumatic Checkout Ch A/B
47	Pneumatic Checkout Ch A and Ch B
51/52	Controller Checkout Ch A/B
71/72	PROM Test A/B
75/76	DCU/CIE Self-Disqualification Ch A/B

Table II provides the detailed failure responses for Controller Checkout.



### 3.2.4:1 Failure Response and Redundancy Management

The response to a confirmed failure will be to disqualify the failed element and all other functions or devices whose monitoring and failure detection are prevented by the failure.

The function of redundancy management is to ensure that all such secondary disqualifications are implemented as part of the response to the primary failure and disqualification. In specific cases a tertiary, third order, disqualification is required as a result of secondary disqualifications. Such tertiary responses will be satisfied in all cases but they may be executed through subsequent monitoring, and are not required to be part of the primary response.

When a failure is reported under a given ID, its effect on mission phase/mode will include all the consequential disqualifications so as to ensure both fail-operational and fail-safe performance. The phase/mode response ultimately required should be reached in the earliest practical time. However, it may be subsequent to the primary response if software simplicity or efficiency results, as long as the overall response time is within that allowed the controller.

Multiple and extraneous failure reporting will be minimized as follows:

- (a) A given Failure Identification Word will be reported only once until acceptance of a Controller Reset command, with the following exceptions:
  - (1) Output Electronics Non-Disqualifying Ch A/B, (FID 7/10, all delimiters)
  - (2) Shutdown Limit Monitor (FID 113, all delimiters, and FID 13, delimiters 413 and 414, during delayed shutdown)
  - (3) RVDT Miscompare (FID 15, delimiters 110-150)
  - (4) FASCOS Shutdown Limit Monitor (FID 117, all delimiters)
  - (5) FASCOS Shutdown Limit Exceeded (Monitor Only Option; FID 17, all delimiters)
  - (6) Switch VRC Commanded (FID 20, delimiter 100)
  - (7) Component Checkout (FIDs 22, 34, 135, 35, 136, 36, 43, 44, 45, 46, 47, 51, 52; all delimiters)
  - (8) Power Recovery (FID 37, all delimiters)

3.2.4:1 Failure Reporting and Redundancy Management  
(Continued)

- (9) Command Voting Failures (FID 42, all delimiters).
- (10) DCU/CIE Self-Disqualification Ch A/B, PRI in DCU already disqualified (FIDs 75/76, delimiter 632)
- (b) Sensors of a parameter can be monitored for more than one function, and each function has specific sensor qualification criteria. If any qualification test should permanently disqualify a sensor, that sensor will be permanently disqualified for all functions and only the first disqualification will be reported. MCC Pc, however, is an exception. Mcc Pc qualification for Control and Ignition Confirmation is independent of qualification for Shutdown Limit monitoring.
- (c) [IR989] Secondary disqualifications shall be implemented under the primary FID and only the primary failure shall be reported.
- (d) When several monitoring functions which are not directly related can be affected by the same hardware failure, the relative timing of the monitoring will be selected so that the failure with the most secondary disqualifications will be confirmed first. The report of that failure will then preclude further failure reporting related to that hardware failure. This is a design goal to be balanced against simplicity, efficiency, and clarity of software design.
- (e) Once a failure is reported, monitoring will be suspended until restored by a Controller Reset command, with the following exceptions:
  - (1) Output Electronics Non-Disqualifying Ch A/B, (FID 7/10, all delimiters)
  - (2) Shutdown Limit Monitor (FID 113, all delimiters, and FID 13, delimiters 413 and 414, during delayed shutdown)
  - (3) RVDT Miscompare (FID 15, delimiters 110-150)
  - (4) FASCOS Shutdown Limit Monitor (FID 117, all delimiters)
  - (5) FASCOS Shutdown Limit Exceeded (Monitor Only Option; FID 17, all delimiters)

3.2.4:1 Failure Response and Redundancy Management  
(Continued)

- (6) Thrust Limiting (FID 20, delimiter 3)
- (7) Report Pc Ref as MCC Pc Control Value in VDT (FID 20, delimiter 4)
- (8) Switch VRC Commanded (FID 20, delimiter 100)
- (9) Component Checkout (FIDs 22, 34, 135, 35, 136, 36, 43, 44, 45, 46, 47, 51, 52; all delimiters)
- (10) Power Recovery (FID 37, all delimiters)
- (11) Command Voting Failures (FID 42, all delimiters)
- (12) DCU/CIE Self-Disqualification Ch A/B, PRI in DCU already disqualified (FIDs 75/76, delimiter 632)

3.2.4:2 Failure Reporting

[IR990] Failure data shall be entered in the VDT such that the transmitted VDT always contains a non-ambiguous report of detected failures.

The VDT failure entries are:

(a) Failure Identification Word

[IR991:587;1] The 7 MSBs of a Failure Identification Word shall be the Failure ID, and the 9 LSBs of a Failure Identification Word shall be the Failure Delimiter. [IR992:587;1] Values of these fields shall be as specified in Table I.

The Failure ID identifies the generic function or type of function affected. The Failure Delimiter indicates what particular element or device has failed.

3.2.4:2 Failure Reporting (Continued)

The Failure Identification Word defines 4 VDT words:

(1) VDT Word 5

[IR993:587;1] VDT Word 5 shall contain the Failure Identification Word which corresponds to the most recent confirmed failure detected prior to initiation of VDT transmission.

(2) VDT Words 100-102

[IR993:4181;1] VDT Words 100-102 shall contain the Failure Identification Words which correspond to the first three confirmed failures during the current VDT cycle. The Failure Identification Words in VDT Words 100-102 are accompanied by Failure Parameter values per (d) and 3.2.4:3.

(b) Inhibit Control Failure Response (I-response) Count (Selectable VDT Word 90)

The I-response count is incremented for each I-response, per Table I. It is decremented for each Resume command while an I-response is in effect. Controller Reset zeros the count. See 3.2.4:4(r) and 3.2.3:1.1.1.

(c) Failure Counter (Selectable VDT Word 91)

[IR993:2361;3] The Failure Counter shall contain an accumulated count of the FIDs reported since the last Controller Reset command. The Failure Counter will be reset to zero upon Controller Reset, per 3.2.3:1.1.1.

(d) Failure Parameter Values (VDT Words No. 103-105)

[IR995] The Failure Parameter Words shall contain the data or parameter value that failed the monitoring test and caused the element or device to be reported as failed.

For failures detected in OE Register monitoring (including storage and on/off registers) via the Digital Self-Test Word inputs, the Parameter Value word will identify those bits of the reported register that have been newly confirmed as failed in the current self-test input.

3.2.4:2 Failure Reporting (Continued)

For failures detected in Sensor Checkout and Calibration, the 6 LSBs of the failed parameter value will indicate the number of out-of-limit values (up to 64 decimal). Failure Parameter Words will be reset to zero upon Controller Reset, per 3.2.3:1.1.1.

(e) Engine Status Word, Self-Test Status Field  
(VDT Word 3)

The Self-Test Status field of the ESW will indicate one of the following, per Table VIII.

- (1) Engine OK
- (2) Major Component Failed
- (3) Shutdown Limit Exceeded

Engine OK is the nominal status. Failures which would change the status to Major Component Failed (MCF) or Shutdown Limit Exceeded (SLE) are indicated in Table I.

[IR1000:3364;1] If Major Component Failed and Shutdown Limit Exceeded exist concurrently, the Self-Test Status shall be Shutdown Limit Exceeded.

Shutdown Limit monitoring (3.2.3:5.3.1) and FASCOS Limit monitoring (3.2.3:5.4.1) will post an SLE when limits are exceeded. [IR1000:3828;1] If this monitoring negates the SLE because limits are no longer exceeded, the ESW shall revert to MCF.

Acceptance of a Controller Reset command will restore the Engine OK status from Shutdown Limit Exceeded or Major Component Failed. [IR1002:4579;1] An MCF shall also be cleared by a Resume command if the following are true:

- (4) All MCFs posted have been resumable (e.g., no non-resumable MCFs).
- (5) The current phase is either Checkout, Start Preparation, or the Standby mode of Post Shutdown.
- (6) When the Resume command is accepted, either the I-response count is zero or it will be decremented to zero because of the Resume command.

3.2.4:3 Failure Lists

[IR1003] Failure Identification Words and Failure Parameter Values of confirmed failures shall be reported in their respective lists, previously described in 3.2.4:2. The sequencing of entries in these lists will be as follows:

- (a) [IR1004] The failure data of the first confirmed failure in a VDT transmission cycle (interval) shall be entered at the start of the lists, Failure Identification Word in VDT Word 100 and Failure Parameter Value in VDT Word 103. [IR1005] VDT Words 101 and 104 shall be set to zero to terminate the lists.
- (b) [IR1006] The Failure Identification Word and Failure Parameter Value for the second confirmed failure in the VDT cycle shall be entered in VDT Words 101 and 104 respectively. [IR1007] VDT Words 102 and 105 shall be set to zero for the second confirmed failure. [IR1008] The Failure Identification Word and Failure Parameter Value for the third confirmed failure in a VDT transmission cycle shall be stored in VDT Words 102 and 105 respectively; however, no VDT Word is cleared for the third failure.
- (c) [IR1009] Failure Identification Word and Failure Parameter Value data of confirmed failures beyond the third in a VDT cycle shall not be entered in the lists.
- (d) The Failure Identification Word of the most recent confirmed failure detected prior to initiation of VDT transmission will be entered in VDT Word 5.
- (e) [IR1011] If no new confirmed failures have been detected in the current VDT transmission cycle, the lists and VDT Word 5 shall remain unchanged.
- (f) Acceptance of a Controller Reset command will clear the lists per 3.2.3:1.1.1.
- (g) [IR1012] An additional circular list (FID buffer) of thirteen failure reports shall be retained. [IR1013] This list shall contain the following:
  - (1) Failure Identification Word
  - (2) Failed Parameter Value
  - (3) Time Reference (except during component checkout when Checkout Step Number is used in place of Time Reference).

### 3.2.4:3 Failure Lists (Continued)

This list will also be cleared on acceptance of a Controller Reset command. [IR1014] Entries to this list shall be made in a circular manner, into ascending locations until the buffer is full, then repeating from the beginning of the list. [IR1015] The next available entry shall be indicated by entering an all-zero bit pattern into that entry location.

For purposes of these requirements, the VDT transmission cycle is defined to start (and end) at the time scheduled for latest entry of a Failure Identification Word in VDT Word 5, in preparation for transmission initiation (see 3.2.4:2). [IR1016:1612;1] The Operational Program shall ensure that the lists are transmitted as non-ambiguous sets of data.

### 3.2.4:4 Failure Response

Response to the various failures is a function of the engine phase as indicated in Table I.

All failures will be reported per 3.2.4:2, except those for which a DSD response is indicated. The types of responses are:

(a) CR: Command Rejection #1

[IR1020:2422;1] The following commands shall henceforth be rejected: Purge Sequence 1, Purge Sequence 2, Purge Sequence 3, Purge Sequence 4, and Terminate Sequence (3.2.2:1.3).

(b) CR2: Command Rejection #2

[IR1021:2422;1] The following commands shall henceforth be rejected: Purge Sequence 1, Purge Sequence 2, Purge Sequence 3, and Purge Sequence 4, (3.2.2:1.3).

(c) D: Disqualification of indicated parameter(s)

[IR1022:1608;1] If the reported Failure Identifier is a DCU, OE, IE, or Servoactuator failure then that device shall be disqualified. [IR1022:1843;1] If the reported Failure Identifier is a sensor parameter (MCC PC for instance) then that parameter shall be disqualified.

(d) D\*: Disqualification for Engine Ready monitoring

[IR1023:1608;1] The sensor parameter shall be removed from the list of parameters required for Engine Ready.

3.2.4:4 Failure Response (Continued)

- (e) D\*\* : Disqualify In-Channel OE in Shutdown

[IR1023:2248;1] If the Emergency Shutdown Solenoid fails ON prior to Shutdown, the corresponding OE channel shall be disqualified upon entry into Shutdown. [IR1023:2248;2] If the Emergency Shutdown Solenoid fails ON during Shutdown, the corresponding OE channel shall be disqualified within a major cycle.

- (f) DF : Discontinue Monitoring Function/Command Off

[IR1023:2368;1] If an On/Off device fails, monitoring shall be discontinued and the function shall be commanded Off.

- (g) DM : Discontinue Monitoring Function/Do Not Command Off

[IR1023:2368;2] If an On/Off device fails, monitoring shall be discontinued, but the command shall not be commanded Off.

- (h) DSD : DCU Self-Disqualification

In-channel DCU is to perform self-disqualification per 3.2.1:6.1.

- (i) E : Emergency Shutdown solenoid deenergized

[IR1025:2248;1] The Emergency Shutdown Solenoid shall be deenergized immediately.

- (j) E\* : Emergency Shutdown Solenoid to be deenergized when Shutdown is entered.

[IR1026:2248;1] The Emergency Shutdown Solenoid shall be deenergized in the first major cycle of Shutdown when shutdown does occur.

- (k) EL : Electrical Lockup

[IR1027:1608;1] The Electrical Lockup mode defined in 3.2.3:1.7.1 shall be entered, provided Hydraulic Lockup is not in effect. [IR1027:2049;1] If the Hydraulic Lockup mode is in effect, this response shall not cause a change of engine phase/mode.



3.2.4:4 Failure Response (Continued)

(l) FD: Fixed Density

[IR1027:4181;1] The response shall be entered into the Fixed Density mode, as described in 3.2.3:1.7.4. All subsequent computations will use constant fuel density values as specified in Table XVI.

(m) FID 5: Failure Identification Word 5

The report and response is given under FID 5.

(n) FID 6: Failure Identification Word 6

The report and response is given under FID 6.

(o) FID 75: Failure Identification Word 75

The report and response is given under FID 75.

(p) FID 76: Failure Identification Word 76

The report and response is given under FID 76.

(q) HL: Hydraulic Lockup

[IR1028:2815;1] The response shall initiate Hydraulic Lockup mode defined in 3.2.3:1.7.2. Subsequent engine shutdown will be Pneumatic Shutdown unless a T-response is invoked by Propellant Drop Monitoring.

(r) I: Inhibit Control Failure Response (I-response)

This response can occur during the Checkout and Start Preparation phases. The effect of an I-response during Component Checkout is specified in 3.2.3:2.3 and its subsections.

[IR1029:1608;1] During Start Preparation, the I-response shall result in continuation of the ongoing mode, but shall prevent sequencing to the next Start Preparation mode or Start Phase. [IR1029:2817;1] Exceptions to this requirement shall be made for reentry of Purge Sequence Three and reversion to Purge Sequence Four.

Commands which initiate certain engine operations will be rejected when an I-response is in effect, per Table V.

[IR1029:4702;1] The standby DCU shall not report an I-response during the Start Preparation phase.

3.2.4:4 Failure Response (Continued)

[IR1029:1934;1] The I-response count (VDT word 90) shall be incremented once each time a failure occurs that causes an I-response, per Table I. Whenever the I-response count is greater than zero, an I-response is considered to be in effect, and will cause command rejection per Table V.

[IR1029:1934;2] A Resume command shall decrement the I-response count by one only if an I-response is in effect. [IR1029:1934;3] If the I-response count decrements to zero, the I-response shall no longer be in effect, thus allowing resumption of interrupted checkout sequences, and acceptance of affected vehicle commands.

Execution of a Controller Reset command will cancel the I-response failure condition and set the I-response count to zero.

Engine Ready Monitoring of the MOV or MFV Hydraulic Temperature will be bypassed, per 3.2.3:5.1, if both sensors of that parameter fail and the start sequence is continued by a Resume command.

If the engine phase/mode is Engine Ready, reversion to Purge Sequence Four will occur using the Sequence of Table X, Part H (Purge Sequence 4 Rollback). An exception to this is if Purge Sequence Three is specified.

Monitoring of the Antiflood Valve Position for Ignition Confirmation will be bypassed, per 3.2.3:5.2, if both channels fail in Start Preparation and the sequence is continued by Resume command.

- (s) I\*: I-response and remain in Component Checkout

This response is applicable to failures detected during Component Checkout which will not cause an abort to Checkout Standby. [IR1029:4526;1] This response is similar to the I-response noted above, but the current Component Checkout mode shall not change as a consequence of the I-response.

- (t) M: Monitor On/Do Not Command Off

[IR1029:2368;1] If an On/Off device fails, monitoring for the failed On condition shall continue and the function shall not be commanded Off.

3.2.4:4 Failure Response (Continued)

(u) MF: Monitor On/Command Off

[IR1029:2368;2] If an On/Off device fails, monitoring for the failed On condition shall continue and the function shall be commanded Off.

(v) P3: Reentry of Purge Sequence 3

[IR1030:2817;1] If engine phase/mode is Purge Sequence Four or Engine Ready, Purge Sequence Three shall be reentered following the I-response processing specified in (r).

(w) PS: Pneumatic Shutdown

[IR1031:1608;1] This response shall cause engine shutdown via the fail-safe Pneumatic Shutdown sequence as defined in Table XIV. [IR1031:1608;2] All igniters, fail-safe servoswitches, and solenoids shall be deenergized in the same major cycle that the failure (causing the response) was detected. [IR1031:1608;3] All igniters, fail-safe servoswitches, and solenoids shall again be deenergized in the first major cycle of Pneumatic Shutdown. This is done to assure that the deenergized state is maintained in the event that intervening processing had reenergized an On/Off device.

If a PS-response is requested in Post Shutdown Standby mode, the sequence of Table XIV may be limited to the response of step 8 for actuator disqualification and monitoring. The output devices will then be maintained in the Post Shutdown Standby configuration.

(x) PS/HL: Pneumatic Shutdown/Hydraulic Lockup

[IR1032:3070;1] If the engine phase is Start the response shall be Pneumatic Shutdown, otherwise the response shall be Hydraulic Lockup.

3.2.4:4 Failure Response (Continued)

(y) PS/PS: Pneumatic Shutdown/Pneumatic Shutdown

[IR1033:1608;1] Pneumatic Shutdown shall be performed if ignition is not confirmed, otherwise Pneumatic Shutdown shall be performed when shutdown occurs.

(z) PS/S: Pneumatic Shutdown/Hydraulic Shutdown

[IR1033:2248;1] If Hydraulic Lockup is in effect or RVDT comparison test has failed, Pneumatic Shutdown shall be performed, else Hydraulic Shutdown shall be performed.

(aa) PS/S\*: Pneumatic Shutdown/Delayed Hydraulic Shutdown

[IR1033:5469;1] If Hydraulic Lockup is in effect or RVDT comparison test has failed, Pneumatic Shutdown shall be performed, else Hydraulic Shutdown shall be performed. [IR1033:5469;2] For failures occurring between Start + 0.80 sec and Start + 1.48 sec, Hydraulic Shutdown shall be delayed until Start + 1.50 sec.

(ab) R: Report Only

[IR1033:2248;2] This response shall be to report the failure in the VDT.

(ac) S: Hydraulic Shutdown

[IR1035:5796;1] This response shall cause engine shutdown by initiating the Shutdown Phase.  
[IR1035:5796;2] Hydraulic Shutdown sequencing shall then be accomplished per Table XIII.

(ad) S/EL: Shutdown/Electrical Lockup

[IR1035:5502;1] If the engine phase is Start with no prior RVDT miscompare, the response shall be Hydraulic Shutdown. [IR1035:5502;2] If the engine phase is Start with a prior RVDT miscompare, the response shall be Pneumatic Shutdown.  
[IR1035:5502;3] If the engine phase is Mainstage the response shall be Electrical Lockup.

3.2.4:4 Failure Response (Continued)

(ae) S\*/EL: Delayed Shutdown/Electrical Lockup

[IR1035:5502;4] If the engine phase is Start with no prior RVDT miscompare, the response shall be Hydraulic Shutdown. [IR1035:5502;5] If the engine

phase is Start with a prior RVDT miscompare, the response shall be Pneumatic Shutdown.

[IR1035:5502;6] If the engine phase is Mainstage the response shall be Electrical Lockup. [IR1035:5502;7]

For failures occurring between Start + 0.80 sec and Start + 1.48 sec, Hydraulic Shutdown shall be delayed until Start + 1.50 sec.

(af) T: Terminate Checkout Sequence (T-Response)

[IR1038:1608;1] Detection of propellants in the engine shall cause termination (abort) of any checkout or FRT sequence that may be in progress or commanded.

[IR1038:3300;1] For either FRT configuration this response shall deactivate the FRT mode such that real engine parameter values are used for all functions.

[IR1038:2419;2] In addition this response shall secure the engine by performing Terminate Sequence (Table XV, Part A). After executing Terminate Sequence the engine phase/mode will be Post Shutdown Standby and the configuration will remain unchanged.

[IR1038:1608;2] This response (T-Response) shall remain in effect until acceptance of a Controller Reset command.

A T-Response will cause rejection of most commands unique to Ground Checkout configuration or unique to the FRT configurations. It will not affect acceptance of commands acceptable in the Flight configuration. [IR1038:2422;1] Table V gives an explicit list of commands that shall be rejected when a T-Response is in effect.

(ag) TO: DCU B Takeover

[IR1039:1608;1] DCU B shall takeover as specified in 3.2.1:9.1.

### 3.2.5 Adaptation and Operational Data Constants

Adaptation and Operational Data Constants are those constants which pertain to engine component or engine performance characteristics. These data will be alterable via Memory Load operations performed in PROM.

#### 3.2.5:1 Adaptation Data Constants

The input signals to the controller are the outputs of transducers that measure parameters of the engine or its devices. They are, therefore, functions of the sensed parameters and are defined by coefficients that represent the transducer scale factors. All inputs are first-degree functions of the measured parameters except temperatures which are represented by a fourth-degree function.

[IR1063:6164;1] The scaling coefficients listed in Table XXVIII shall be used as the nominal values. [IR1064:3764;1] When using these scaling coefficients the Operational Program shall have the capability of accommodating the full range given for each sensor.

These coefficients, with exception of those for pressure parameters, can be changed via Memory Load to compensate for errors in individual sensors and are designated as Adaptation Data Constants.

During Sensor Checkout, the scaling coefficients for pressure sensors are calculated using calibration constants,  $K_a$  and  $K_{g0}$ . These calibration constants are designed as Adaptation Data Constants.

[IR1067:3764;1] In addition to the coefficients listed in Table XXVIII, the Vehicle Data Table ID Word (1) and Main Engine Controller ID shall be Adaptation Data Constants.

[IR1068] A dedicated location in main memory shall be created to identify a main engine controller. [IR1069:4015;1] Bits 15-12 of this location shall hold an octal number from 0-17 where a 5 will identify a F-type controller, and all other Block II controller types shall be designated with a code of 0. Codes 1, 2, and 3 have been used by Block I and are reserved. [IR1069:2001;2] Bits 11-0 of this location shall hold an octal number from 0000-7777, the octal equivalent of the decimal (numerical) part of the MEC identification number.

3.2.5:2 Operational Data Constants

[IR1070] Other quantities which may require changes to accommodate the performance characteristics of the engine shall be designated as Operational Data Constants. Like Adaptation Data Constants, Operational Data Constants will be alterable via memory load while cycling in PROM. [IR1072] Except during Memory Load while cycling PROM, the Operational Data Constants shall remain fixed and unalterable. The documentation will refer to Operational Data Constants as constants.

[IR1073:6239;1] The following shall be included as Operational Data Constants:

- (a) All quantities making up the profiles of engine sequences
- (b) Limits defining Engine Ready
- (c) Limits for comparison and reasonableness monitoring of sensors
- (d) Shutdown Limit Monitoring (Redline) Limits
- (e) Limits for monitoring the engine purge system
- (f) VDT selectable entries
- (g) Engine-dependent Time Delays
- (h) FASCOS limit monitoring start time
- (i) Limits For Vibration Limit Exceeded
- (j) Option for FASCOS Monitoring (reference Table I):

[IR1073:6239;2] One FASCOS option shall be selected from the following list:

- (1) Fully Active - All vibration channel monitoring will be performed. The failure responses will include any disqualifications along with the posting of inhibits, MCFs or SLEs.
- (2) Monitoring Only - All vibration channel monitoring will be performed. The failure responses will be report only; no inhibits, MCFs or SLEs will be posted.
- (3) Bypass - All vibration channel qualification and redline monitoring will be bypassed. No failure responses will be reported for any FASCOS-related parameter, except in Sensor Checkout.

3.2.5:2 Operational Data Constants (Continued)

- (k) Vibration Limit Qualification strike count limit  
(3.2.3:4.3.2(a))
- (l) FASCOS Limit Monitor strike count limit (3.2.3:5.4.1)
- (m) The Stop DCU command acceptance indication
- (n) Selection criteria for choosing which channel of the Controller Internal Pressure and which channel of the Controller Internal Temperature that will be reported in the VDT. Reference Table VI Note 16.
- (o) The 20 msec VDT Switch (3.3.4:10)
- (p) Data which is engine performance dependent yet engine hardware independent
- (q) Single Command Channel Shutdown Enable timer  
(3.2.2:1.2(b)).
- (r) Times and MCC Pc value associated with the implementation of shutdown delays during Start.



### 3.3 Design Requirements

[IR1533:2000;1] Except where noted, the detailed requirements of this section shall apply to the Operational Program in both DCU A and DCU B.

#### 3.3.1 Development Requirements

The Operational Program will be developed using modern design techniques, defined in a development plan.

#### 3.3.2 Design Documentation Requirements

The Operational Program will be documented in accordance with approved design guidelines and standards.

Every variable will be defined in terms of at least the following attributes:

- (a) Data Item Name
- (b) Description
- (c) Set By
- (d) Used By

#### 3.3.3 Coding Standards

The Operational program will be coded in "C" and/or MC68000 assembly language.

Source code will conform to approved standards and guidelines.

#### 3.3.4 Design Restrictions

##### 3.3.4:1 Spare Memory and Time

##### 3.3.4:1.1 Spare Memory

It is a design goal to deliver to the customer an Operational Program that will not use more than 51.2k words (80%) of available RAM main memory.

[IR1537] All unused locations shall contain the Illegal instruction as defined in the MC68000 Programmer's Reference Manual.

[IR1538:4597;1] Addresses \$FFFC, \$FFFD, \$FFFE, \$FFFF, \$FFFFFC, \$FFFFFD, \$FFFFFE, and \$FFFFFF shall be unused for purposes other than memory load via PROM, memory readout, by the SCP Comparator Test of 3.2.3:2.3.5:1, and by the Failure Data Recorder Test of 3.2.3:2.3.5:28.

3.3.4:1.2 Spare Time

[IR1538:6191;1] The nominal major cycle processing time in Start, Mainstage, or Shutdown phase shall not exceed 18 msec in the Operational Program delivered to the customer.

3.3.4:2 Memory Locations Dedicated to PROM

[IR1538:1386;2] The following memory locations shall be dedicated for PROM use, as specified.

<u>Location</u>	<u>Contents</u>
\$0400	Pointer to start address of Sum Check Address Table (SCAT)
\$0404	Start Address for RAM execution (after Exit PROM command)
\$FF00-\$FFFB	Scratch Pad Area (for PROM)

3.3.4:2.1 Sum Check Address Table (SCAT)

[IR1538:2676;1] A sufficient number of contiguous memory locations, to be determined by Design, shall be reserved for the SCAT, starting at a location other than \$0.

[IR1538:1131;4] The SCAT shall consist of pairs of 32-bit addresses to be interpreted as sumcheck start and end addresses, where the end address is always greater or equal to the start address. [IR1538:1131;5] The arithmetic sum (sumcheck) of the contents of all memory locations between and including each start and end address shall be \$A5A5.

[IR1538:1131;6] The last address pair in the SCAT to be sumchecked shall be followed by a 32-bit word containing zero. (If the first entry in the SCAT contains zero, no sumchecks will be performed).

[IR1538:2676;2] A total memory load shall include a SCAT which will enable PROM to sumcheck RAM Main Memory. [IR1538:4672;1] The addresses to be sumchecked via this initial SCAT shall include all of RAM Main Memory, but shall exclude address locations \$000000 through \$00010B and \$00FF00 through \$00FFFF. The first address range contains all the exception vector locations used by PROM, while the second range corresponds to the PROM Scratch Pad Area. Upon entry into RAM from PROM, the SCAT will be modified to disable the RAM Sum Check function, per 3.2.1:1.3.

3.3.4:3 RAM Integrity

[IR1538:4012;1] The following memory locations shall be assigned the values as shown below:

<u>Location</u>	<u>Contents</u>
\$FEFE	\$3333
\$FFFFFFA	\$CCCC

The contents of the lower memory location is the complement of the contents of the upper memory location.

In the event of a suspected power transient or power loss the integrity of RAM can be assessed by performing a Memory Readout of the fixed locations described above and verifying the fixed contents.

3.3.4:4 Overlays

Software overlays are prohibited.

3.3.4:5 Verification of Loaded Program

Verification that the loaded software configuration and individual routines are correct to the delivered Operational Program documentation is the responsibility of the (vehicle) controlling system. It will be assumed that the contents of the entire memory are verified with the following exceptions:

- (a) Data and locations individually excluded under paragraph 3.2.
- (b) Sensor calibration coefficients computed per paragraph 3.2.3:2.3.1 when not overwritten as Adaptation Data Constants.
- (c) Locations designated for temporary variables or for status/logic indicators that are modified by the Operational Program when cycling.

[IR1538:2638;1] To assist in this verification, a Memory Compare Table shall be included in the Operational Program that defines those regions of memory that do not change during execution of the software. [IR1538:2638;2] This table shall consist of pairs of 32-bit addresses that indicate start-end regions of memory to be compared. [IR1538:2638;3] The last address pair in the table shall be followed by a 32-bit word containing zero.

#### 3.3.4:6 Exception Vector Handling

[IR1541] Exception processing routines shall not change memory locations, set interrupt masks or initiate any output from the computer except where the memory locations, interrupt masks or outputs are specifically designed and designated to be used by the exception processing routine.

[IR1543] The contents of all address and data registers shall be saved upon entering the exception processing routine. This is to maintain the original state of the processor. [IR1544] Upon completion of exception processing the contents shall be restored and normal processing shall resume.

#### 3.3.4:7 Computational Precision

Data scaling of each intermediate result and the use of double-precision processing will be used to prevent degradation of significance and to provide the needed resolution of output data. The precision of processing will be selected to maintain the computation errors smaller than the least resolution bit of output data or the least accurate bit of input data as applicable. Ground rules for typical parameters are as follows:

- (a) Control Loop Equation processing will assure data resolution and significance compatible with those of VEEI Main Chamber Pressure Level Command.
- (b) Propellant Valve Control processing will assure data resolution and significance compatible with valve position commands transmitted to the Output Electronics.
- (c) Monitoring Function processing will assure data resolution and significance compatible with the applicable monitoring limits or the accuracy indicated in the VDT, Table VI, whichever is more exacting.

#### 3.3.4:8 Adaptation & Operational Data Design Constraints

[IR1552:1677;1] All data classified as either Adaptation or Operational Data (3.2.5) shall have fixed locations independent of compilation or load processes.

3.3.4:9 Special Patch Software Hook

[IR1552:1651;1] For purposes of a potential special patch, the Operational Program shall have a software hook incorporated.

[IR1552:1651;2] This hook shall consist of 20 usec of the nominal major cycle path and 150 words of contiguous memory available for the patch.

3.3.4:10 20 msec VDT

[IR1552:1941;1] For purposes of test, a selection of either a 20 or 40 msec duration between initiation of VDT transmissions shall be provided. [IR1552:1941;2] A single data constant (operational data) shall be used to determine the time duration.

#### 4.0 QUALITY ASSURANCE PROVISIONS

This section establishes the procedures which assure that the computer program defined by this specification meets the requirements in sections 3.2 and 3.3 of this specification. This section describes development and formal independent verification.

##### 4.1 Development

[IR1553:2638;1] During software development, reviews of the software design and code shall be conducted per the Programmers' Handbook for the SSME Block II Controller Software.

##### 4.2 Formal Independent Verification

[IR1554] The computer program shall be subjected to independent verification by personnel not directly involved in its design or coding. [IR1555:3162;1] Verification shall be in accordance with the Block II SSMEC Verification Guidelines (RF0001-092).

## 5.0 PREPARATION FOR DELIVERY

Programs and data to be delivered will be identified, marked and shipped per the following requirements.

### 5.1 Object Programs

[IR1560:2638;1] Object code shall be supplied for the Operational Program in the form of a system magnetic tape, along with its corresponding compare image, also in the form of a system magnetic tape. [IR1560:2638;2] The format and organization for these tapes shall be in accordance with the SSME Interface Control Document (ICD-13M15000).

### 5.2 Identification and Marking

[IR1584:2638;1] The identification data applied to the program tape labels shall conform to the Block II SSMEC Software Delivery System Requirements Specification (RHF-0031-001).

### 5.3 Program and Concordance Listing

[IR1585:8;1] Program and concordance listings shall be supplied with each program. [IR1586:8;1] The program listing shall include the object-source listing generated at the time of compile/assembly and the memory link map, load map. [IR1587:8;1] The concordance listing shall include a cross-reference list of all source program symbols. [IR1588:8;1] The listings shall include reference to the program identification number.

### 5.4 Documentation

Rocketdyne will prepare and submit CPCEI specifications in accordance with the Data Requirement Document of the purchase order.

[IR1589:8;1] A letter of transmittal shall accompany each program tape delivery. [IR1590:8;1] This letter shall provide:

- (a) Configuration identification, including the Rocketdyne control numbers.
- (b) Technical definition including, when applicable, changes incorporated since the previous delivery.
- (c) List of waiver items, if any.
- (d) Bill of lading identifying all items: tapes, listings, etc., included in the delivery.

5.5 Acceptance/Engineering Verification Data Package

The Acceptance/Engineering Verification Package will be provided as specified in the Data Requirement Document of the purchase order as to contents and timing of transmittal.

5.6 Exterior Packaging

Delivered items will be packaged in substantial commercial exterior containers appropriate to the items and constructed to ensure acceptance by common carriers at lowest rate for safe transportation to the point of delivery.



6.0 NOTES6.1 List of Acronyms and Abbreviations

AC	Alternating Current
A/D	Analog to Digital Converter
ADPFI	Alternate DCU Power Failure Interrupt
AFV	Antiflood Valve
BCH	Bose, Chaudhuri & Hocquenghem
BERR	Bus Error
bit	Binary digit
C/O	Checkout
CATP	Controller Acceptance Test Program
CCST	Scheduled position of the CCV
CCV	Chamber Coolant Control Valve
CHK	Check Register Against Bounds (MC68000 instruction and exception)
CIE	Computer Interface Electronics
CIE A	Computer Interface Electronics Channel A
CIE B	Computer Interface Electronics Channel B
CPC	Computer Program Component
CPCEI	Computer Program Contract End Item
CPU	Central Processing Unit
CR	Command Rejection
D/A	Digital to Analog Converter
DC	Direct Current
DCU	Digital Computer Unit
DCU A	Digital Computer Unit Channel A
DCU B	Digital Computer Unit Channel B
DLIM	Delimiter
DPM	Dual Port Memories
DTACK	Data Transfer Acknowledge
EDW	Engine Data Word
EL	Electrical Lockup
ESW	Engine Status Word
FASCOS	Flight Accelerometer Safety Cut-Off System
FBV	Fuel Bleed Valve
FC0	Function Code Output 0 (MC68000)
FC1	Function Code Output 1 (MC68000)
FC2	Function Code Output 2 (MC68000)
FD	Fixed Density

6.1 List of Acronyms and Abbreviations (Continued)

FDR	Failure Data Recorder
FID	Failure ID
FPB	Fuel Preburner
FPOV	Fuel Preburner Oxidizer Valve
FPST	Scheduled position of the FPOV
FRT	Flight Readiness Test
FRT-1	Flight Readiness Test 1
FRT-2	Flight Readiness Test 2
FS	Full Scale
GN <sub>2</sub>	Gaseous Nitrogen
GOX	Gaseous Oxygen
gpm	Gallons Per Minute
Grms	Gravitational acceleration Root Mean Squared
GSE	Ground Support Equipment
He	Helium
hex	Hexadecimal
HI	Honeywell Incorporated
HL	Hydraulic Lockup
HPFP	High Pressure Fuel Pump
HPFT	High Pressure Fuel Turbine
HPOP	High Pressure Oxidizer Pump
HPOT	High Pressure Oxidizer Turbine
hz	Hertz
ID	Identification
IDSR	Inter-DCU Status Register
IE	Input Electronics
IE A	Input Electronics Channel A
IE B	Input Electronics Channel B
IE DPM	Input Electronics Dual Port Memories
I/O	Input/Output
IMSL	Intermediate Seal
IPL0	Interrupt Priority Line 0 (MC68000)
IPL1	Interrupt Priority Line 1 (MC68000)
IPL2	Interrupt Priority Line 2 (MC68000)
khz	Kilohertz

6.1 List of Acronyms and Abbreviations (Continued)

LDA	Latching Digital to Analog
LL	Lower Limit
LOX	Liquid Oxygen
LPFP	Low Pressure Fuel Pump
LPFT	Low Pressure Fuel Turbine
LPOP	Low Pressure Oxidizer Pump
LPOT	Low Pressure Oxidizer Turbine
LSB	Least Significant Bit
LVDT	Linear Variable Differential Transformer
ma	Milliamps
Max	Maximum
MCC	Main Combustion Chamber
MCC Pc	Main Combustion Chamber, Pressure in the Chamber
MCF	Major Component Failed
MEC	Main Engine Controller
MFST	Scheduled position of the MFV
MFV	Main Fuel Valve
min	Minute
Min	Minimum
MOST	Scheduled position of the MOV
MOV	Main Oxidizer Valve
MPU	Microprocessing Unit (MC68000)
MR	Mixture Ratio
M/S	Mainstage
MSB	Most Significant Bit
msec	Millisecond
MUX	Multiplexer
mv	Millivolts
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
nsec	Nanosecond
OBV	Oxidizer Bleed Valve
OE	Output Electronics
OE A	Output Electronics Channel A
OE B	Output Electronics Channel B
OPB	Oxidizer Preburner
OPOV	Oxidizer Preburner Oxidizer Valve
OPST	Scheduled position of the OPOV

6.1 List of Acronyms and Abbreviations (Continued)

PBD	Power Bus Down status bit
PBP	Preburner Pump
PC	Chamber Pressure
PFI	Power Failure Interrupt
POI	Power Off Indicator
pps	Pulses Per Second
PRC	Pulse Rate Converter
PRI	Power Recovery Interrupt
PROM	Programmable Read Only Memory
PS	Pneumatic Shutdown
PS/D	Post Shutdown phase
PSE	Power Supply Electronics
psi	Pounds per Square Inch
psia	Pounds per Square Inch Absolute
R	Rankine
RAM	Random Access Memory
RCFI	Redundant Computer Failure Interrupt
RIV	Recirculation Isolation Valve
rms	Root Mean Square
RPL	Rated Power Level
rpm	Revolutions Per Minute
RTC	Real Time Clock
RVDT	Rotary Variable Differential Transformer
SCAT	Sumcheck Address Table
SCP	Self-Checking Pair
SCPI	Self-Checking Pair Interrupt
SCP-P	Self-Checking Pair Processor
S/D	Shutdown
sec	Second
SEI	Servoactuator Error Indication
SEII	Servoactuator Error Indication Interrupt
SLE	Shutdown Limit Exceeded
SL1/SL2	Solenoid Level One/Two
SP	Start Preparation phase
SQA	Software Quality Assurance
SSME	Space Shuttle Main Engine
SSMEC	Space Shuttle Main Engine Controller
ST	Start phase
TRI	Timing Reference Interrupt

6.1 List of Acronyms and Abbreviations (Continued)

UL	Upper Limit
usec	Microsecond
Vac	Volts Alternating Current
VCC	Vehicle Command Channel
Vdc	Volts Direct Current
VDT	Vehicle Data Table
VDT1A	VDT from DCU A DPM #1
VDT1B	VDT from DCU B DPM #1
VDT2A	VDT from DCU A DPM #2
VDT2B	VDT from DCU B DPM #2
VEEI	Vehicle Engine Electrical Interface
VIE	Vehicle Interface Electronics
Vpp	Volts Peak to Peak
VRC	Vehicle Recorder Channel
VRC DPM	VRC Dual Port Memories
VRCA	Vehicle Recorder Channel A
VRCB	Vehicle Recorder Channel B
VRCA-	
VDT1A	DCU A DPM #1 VDT output on VRCA
VRCA-	
VDT1B	DCU B DPM #1 VDT output on VRCA
VRCB-	
VDT2A	DCU A DPM #2 VDT output on VRCB
VRCB-	
VDT2B	DCU B DPM #2 VDT output on VRCB
Vrms	Volts Root Mean Square
VSPE	Vibration Sensing and Processing Equipment
WDT	Watchdog Timer
WDT1	Watchdog Timer 1
WDT2	Watchdog Timer 2
WDTH	Watchdog Timer Halt interrupt
WDTH1	Watchdog Timer Halt One interrupt
WDTH2	Watchdog Timer Halt Two interrupt

## 6.2 Glossary

\$ When a number is prefixed by a \$ that number will be interpreted to be hexadecimal (per Motorola's notation.)

% When a number is prefixed by a %, that number will be interpreted to be binary (per Motorola's notation.)

When a number is an actuator position or command and is followed by a %, that number will be interpreted to be a percentage of full open or full scale. Full open, full scale, and 100% will be considered equivalent. A full closed command is 0%.

@ When a number is prefixed by a @ that number will be interpreted to be octal (per Motorola's notation.)

Actuator - See Servoactuator

Analog to Digital Converter (A/D)

A mechanism in each IE to convert analog sensor signals into digital signals.

Bose, Chaudhuri & Hocquenghem (BCH)

Coding scheme used to verify the integrity of vehicle commands.

Blueline

A set of limits close to but not exceeding Redline (shutdown) limits. The Blueline is exceeded only when all applicable parameters exceed their Blueline limits.

Bus Error

MC68000 Exception associated with lack of DTACK.

Byte

8 bits (binary digits).

C

The main programming language in which Block II Software is written.

Central Processing Unit (CPU)

In Block II this is the Motorola MC68000 microprocessor.

## 6.2 Glossary (Continued)

### Command Limit

The maximum allowable value of the computed command. It may be a constant or a variable function of another parameter.

### Component Checkout Modes

These modes are Actuator Checkout, Controller Checkout, Engine Leak Detection, Hydraulic Conditioning, Igniter Checkout, Pneumatic Checkout, and Sensor Checkout.

### Controller Component

Refers to the DCU/CIE, IE, OE, and all servoactuators on a channel.

### Cross-Channel

Refers to the DCU and all its associated components on the alternate channel from a DCU (for example DCU B is cross-channel to DCU A; DCU A is cross-channel to DCU B).

### Data transfer acknowledge (DTACK)

An MC68000 signal indicating completion of an input/output data transfer.

### Delimiter (DELIM)

This field is used to uniquely identify a failure given the appropriate FID. A delimiter field is the least significant nine bits of the Failure Identification Word.

### Digital Computer Unit (DCU)

Each contains a self-checking pair of microprocessors, main memories, and PROMs.

### Digital to Analog Converter (D/A)

Used to convert a servoactuator command (digital) from the DCU/CIE to an analog signal for the servoactuator driver.

## 6.2 Glossary (Continued)

### Disable Interrupt

A directive to either raise the current interrupt level to or above the level of the specified interrupt, or to reset (logic 0) the bit corresponding to the specified interrupt in the appropriate CIE interrupt mask register, thus precluding the interrupt.

### Disable Interrupt in the CIE

A directive to reset (logic 0) the bit corresponding to the specified interrupt in the appropriate CIE interrupt mask register, thus precluding input to the CPU.

### Disqualification

The permanent disqualification of a hardware component (See Permanent Disqualification).

### Dual Port Memories (DPM)

See Input Electronics Dual Port Memories or Vehicle Recorder Channel Dual Port Memories.

### Electrical Lockup (EL) Mode

An Engine On degraded mode of operation in which propellant actuator commands are not updated.

### Enable Interrupt

A directive to set (logic 1) the bit corresponding to the specified interrupt in the appropriate CIE interrupt mask register, and to lower the current interrupt level below that of the specified interrupt, allowing the interrupt to occur.

### Enable Interrupt in the CIE

A directive to set (logic 1) the bit corresponding to the specified interrupt in the appropriate CIE interrupt mask register, allowing the interrupt pending indication to be input to the CPU.

### Engine Data Word

A word used to pass engine-related information between DCU A and DCU B, via the Inter-DCU Status Register, as defined in Table XLII.



## 6.2 Glossary (Continued)

### Engine On

Composed of the following engine phases: Start, Mainstage, and Shutdown.

### Engine Operational Phases

Start Preparation, Start, Mainstage, Shutdown and Post Shutdown are Engine Operational phases. The only non-Engine Operational phase is the Checkout phase. Notice: FRT-1 and FRT-2 tests utilize the Engine Operational phases but only simulate Engine operations.

### Fail-Operational

The system continues to operate after a single failure. Refers to state of engine control or servoswitches.

### Fail-Safe

The system remains safe after several failures. Refers to state of engine control or servoswitches.

### Failure Data Recorder (FDR)

A 2K by 48 bit recorder of the last 2K of data, address, and bus control signals, located in the CIE. Its function is diagnostic only.

### Failure ID (FID)

A seven-bit field which identifies a general failure type.

### Failure Identification Word

The Failure Identification Word is made up of two fields: Failure ID and Failure Delimiter. The seven most significant bits contain the Failure ID field, the nine least significant bits contain the Failure Delimiter field. Failure Identification Words will be reported in VDT Data Words 5, 100-102, and the FID buffer.

### Fixed Density (FD) Mode

The mode in which the calculated fuel density is replaced by a constant.

## 6.2 Glossary (Continued)

### Flight Operation

Composed of the following Engine phases: Start Preparation, Start, Mainstage, and Shutdown.

### Flight Readiness Test (FRT)

Generic. In FRT, engine operation is simulated.

### Flight Readiness Test-1 (FRT-1)

Flight Readiness Test, actuators and pneumatic solenoids move as in Flight.

### Flight Readiness Test-2 (FRT-2)

Flight Readiness Test similar to FRT-1, but no fail-safe, fail-operational servoswitches, pneumatic solenoids (except Bleed Valve), and no igniters are to be energized.

### Fuel Preburner Oxidizer Valve (FPOV)

A valve driven by a servoactuator which in turn is controlled by the OEs. This valve is used to control Mixture Ratio.

### Full Closed

Used in the context of a valve command, is a valve position of 0% open.

### Full Open

Used in the context of a valve command, is a valve position of 100% open.

### Halt Exit

A mechanism in the CIE used to enable/inhibit a DCU from responding to an in-channel Reset Channel command.

### High RAM

Addresses \$FF0000 to \$FFFFFF.

### Hold Voltage

Voltage required to hold or keep a solenoid activated once the solenoid has been in the pull-in state.

## 6.2 Glossary (Continued)

### Hydraulic Lockup (HL) Mode

An Engine On degraded mode of operation in which the propellant actuators are hydraulically locked.

### Hydraulic Shutdown

The nominal manner of shutting down the engine.

### I-Response

The Inhibit Control Failure Response reduces the set of acceptable vehicle commands. This response may also stop a checkout sequence.

### Ignition Confirm

Occurs when all parameters monitored for ignition confirmation have passed constraints.

### Immediate Retry

Requires that the reload and reread of the parameter being tested be done before any other successive processing.

### In-Channel

Refers to a DCU and all its associated components from the perspective of that DCU (for example, IE A and OE A, are in-channel to DCU A; and IE B and OE B are in-channel to DCU B).

### In-Control DCU

That DCU/CIE which has control (via the WDTs) of the IEs, OEs, and the VRC Data Switch. Nominally DCU/CIE A is the in-control DCU and DCU/CIE B is the standby DCU. Only one DCU/CIE can be in control at any time.

### Input Electronics Address Counter

A mechanism in each IE that points to the next IE DPM address to be written into by the IE.

### Input Electronics Command Select Switch

Selects which DCU will control the sequencing of both IEs.

## 6.2 Glossary (Continued)

### Input Electronics Data Sequencer

A mechanism in each IE that controls the flow of input data into the IE DPMs.

### Input Electronics Dual Port Memories (IE DPM)

Each CIE contains two Input Electronics Dual Port Memories. Each is dedicated to storing Input Electronics Data from both IEs.

### Input Electronics Range Counter

A mechanism in each IE which contains the number of IE inputs remaining to be made in this IE input request (made by the in-control DCU).

### Interrupt Level Encoder

That part of the CIE which receives signals from 21 pending interrupt sources and encodes these signals into seven priority levels. It also contains the CIE interrupt mask registers.

### Linear Variable Differential Transformer (LVDT)

This device is used as a linear valve position sensor.

### Low RAM

Addresses \$000000 to \$00FFFF.

### Main Chamber Pressure Level Command

The VEEI command used by the controller to command MCC Pc.

### Main Engine Controller Identifier

Adaptation data which identifies the Controller.

### Main Fuel Valve (MFV)

A valve driven by a servoactuator which in turn is controlled by the OEs.

### Main Oxidizer Valve (MOV)

A valve driven by a servoactuator which in turn is controlled by the OEs.

## 6.2 Glossary (Continued)

### Mainstage

An Engine on phase.

### Major Component Failed' (MCF)

An MCF is a failure report transmitted to the vehicle in the Engine Status Word of the VDT. The vehicle potentially uses this data to abort the launch. See Table I for failures to be reported as Major Component Failures.

### Major Cycle

The twenty (20) msec time interval during which all scheduled functions for a computational iteration are processed. That period of time required to perform a nominal cycle of sensor input, scaling, data processing, and engine commands.

### MCC Pc (Measured)

Average of qualified MCC Pc channels.

### MCC Pc (Sensed Value)

This is the value of an MCC Pc Sensor: A1, A2, B1, or B2.

### MCC Pc Channel (Value)

The value of either MCC Pc Channel A or MCC Pc Channel B.

### MCC Pressure (MCC Pc)

Pressure in the Main Combustion Chamber. This measurement is directly related to thrust.

### Minor Cycle

A five (5) msec time interval between successive timing reference interrupts. Four minor cycles comprise a major cycle.

### Mixture Ratio

Ratio of Oxidizer flowrate to Fuel flowrate by weight.

### Multiplexers (MUX)

A many to one hardware switch.

## 6.2 Glossary (Continued)

### On/Off Register

There are three such 12-bit registers in each OE. Each is used to store discrete commands destined for On/Off devices.

### Output Electronics Command Decoder

A mechanism in the OE which directs a digital command to the appropriate devices.

### Output Electronics Command Select Switch

A mechanism in each OE which selects which DCU/CIE is in control by monitoring status of Channel A's WDTs.

### Output Electronics Digital Data Interface

A mechanism in each OE which takes commands from the controlling DCU/CIE and provides control functions to other OE functions.

### Output Electronics Power Control Switch

A mechanism in each PSE which controls the in-channel 2khz excitation and the solenoid, servoswitch, and igniter power supplies. Control is via the in-control DCU/CIE.

### Output Electronics Storage Register

A mechanism in each OE which provides temporary storage for a digital OE command previous to being decoded.

### Oxidizer Preburner Oxidizer Valve (OPOV)

A valve driven by a servoactuator which in turn is controlled by the OEs. This valve is used to control MCC Pc.

### Pc Reference

Rate limited commanded MCC Pc. Used in controlling OPOV, FPOV, and CCV.

### Percent Rated Power Level

A measurement of thrust.

## 6.2 Glossary (Continued)

### Permanent Disqualification

When a hardware component has reached its limit of temporary failures (strikes), the Operational Program follows a set of procedures to make the failed component, and possibly associated components, ineligible for further use (synonymous with Disqualification).

### Pneumatic Shutdown

A fail-safe manner of shutting down the engine.

### Pneumatic Solenoid/Servoswitch/Igniter Power Safety Switch

A mechanism in each OE which provides a high level on/off control of the pneumatic solenoid, servoswitch, igniter and 2khz (RVDT/LVDT) power supplies.

### Pogo (Suppression System)

A mechanism for suppressing oscillations in MCC Pc due to variations in propellant tank pressure.

### Power Bus Down status bit

This bit is located in Input Word six and reports status of cross-channel primary (AC) input power.

### Power Down Matrix

Function in the Output Electronics.

### Power Failure

The temporary or permanent loss of primary (AC) input power. Synonymous with power loss.

### Power Failure Interrupt

An indication of the loss of primary (AC) input power.

### Power Loss

The temporary or permanent loss of primary (AC) input power. Synonymous with power failure.

### Power Recovery Interrupt

An indication that operational power has returned.

## 6.2 Glossary (Continued)

### Power Supply Electronics

Each controller channel contains a power supply that provides power for the in-channel electronics and provides control functions for input power failure and power interruption conditions.

### Power Transient

The loss of primary (AC) input power, followed by return of operational voltages within 59.5 msec.

### Programmable Read Only Memory (PROM)

Fusible link, non-alterable memory.

### Pull-In Voltage

Voltage required to pull-in or energize a solenoid from a non-energized state.

### Qualification

A series of tests performed by the Operational Program to verify the viability of a hardware component and its associated data. These tests must be passed before the component and its data can be considered qualified for use within the system.

### Rankine

A temperature scale which starts at absolute zero. The unit of measurement equals a Fahrenheit degree. Water freezes at 491.69 degrees R.

### Rated Power Level (RPL)

MCC Pc pressure of 3006 psia.

### Readout

Each DCU has the capability to read out and transmit in-channel memory data blocks. There are two types of readout commands: IO Readout, which is used to read out the IE DPM and Input Data Words, and Memory Readout, which is followed by an encoded Starting Address command and is used to read out blocks of the DCU's RAM Main Memory.



## 6.2 Glossary (Continued)

### Real Time Clock (RTC)

A timer which counts down from 4999 to 0 and rolls over. The clock is also used to drive WDT1 and the TRI.

### Redundant Computer Failure Interrupt

An indication to a DCU that a WDT has timed-out in the cross-channel DCU/CIE.

### Redline

A critical Engine Parameter Limit. Values exceeding Redline limits may shut the engine down. Also called a Shutdown Limit.

### Retry

The reload and reread of a parameter (See Immediate Retry).

### Rotary Variable Differential Transformer (RVDT)

Used on actuators to indicate a rotary valve position.

### Self-checking pair processor (SCP-P)

It is composed of 2 MC68000s with individually associated main memories and data/address comparators. Each DCU contains a SCP-P.

### Self-Test

Tests of the hardware performed by the Operational Program.

### Sensor Checkout Group

Group 1 switches allow for sensor calibration and Group 2 switches provide for propellant drop monitoring.

### Servoactuator

The part of the hydraulic actuator which receives the electrical command signal from the controller and converts the signal proportionally into a change in hydraulic fluid flow which turns the actuator shaft. The actuator drives the propellant valve open or closed.

## 6.2 Glossary (Continued)

### Servoswitches

Composed of fail-operational and fail-safe switches in the servoactuators.

### Servovalve

Each OE contains an individual servovalve driver for each actuator. The servovalve driver drives the respective servovalve which in turn moves the actuator (or valve).

### Standby DCU

The DCU/CIE that serves as the backup to the in-control DCU.

### Strike

A detection of a temporary failure on a hardware component.

### Strike Count or Counter

A tally of temporary failures on a particular hardware component or its associated data.

### T-Response

The Terminate Checkout Sequence response occurs when Propellant Drop Monitoring detects inadvertent propellants in the engine. This will invoke the Terminate Sequence mode and cause rejections of most commands unique to Ground Checkout configuration or unique to the FRT configurations.

### Temporary Disqualification

When a hardware component has a temporary failure, that component and its associated data cannot be used by the Operational Program until the component has recovered from the temporary failure.

### Time Reference

Software count of major cycles since being reset.

### Timing Reference Interrupt

Generated once each 5 msec.

## 6.2 Glossary (Continued)

### Unrecoverable Power Failure

The loss of primary (AC) power without the return of operational voltages for more than 59.5 msec duration; or power loss on a channel in which the DCU had been previously disqualified; or power loss during Checkout phase.

### Validated Engine Data Word

An Engine Data Word that has been qualified for use, per 3.2.3:3.1.2:3. Also, see Engine Data Word.

### Valve

A mechanical device which controls the flow of fluids or gases in a channel or pipe. There are valves which open in proportion to a commanded signal (e.g. propellant valves) and valves which can only be commanded closed or open (e.g., pneumatic valves).

### Vehicle Data Table (VDT)

A table of 128 status variables which is transmitted to the vehicle once each 40 msec.

### Vehicle Interface Electronics (VIE)

It provides digital communication link between a CIE and the VEEI channels.

### Vehicle Interface Electronics Command and Data Converter

Three hardware components in the VIE which receive command and memory words from the vehicle.

### Vehicle Interface Electronics Recorder Data Switch

Selects either Channel A or Channel B VRC DPM as the VIE Recorder and Data Converter data source.

### Vehicle Interface Electronics Recorder and Data Converter

Transmits data from the VRC DPM to the VEEI recorder channels.

6.2 Glossary (Continued)

Vehicle Recorder Channel Dual Port Memories (VRC DPM)

The Vehicle Recorder Channel Dual Port Memories are those parts of a CIE used to retain data to be transmitted to the vehicle.

Watchdog Timer (WDT)

Two timers in each CIE. When either of DCU A's WDTs is timed out, control passes to the standby DCU. When either of DCU A's WDTs and either of DCU B's WDTs are timed-out, hardware pneumatically shuts the engine down.

Word

When referencing main memory, a word is 16 bits wide.  
When referencing FDR memory, a word is 48 bits wide.

### 6.3 The Tustin Method

Control functions to be implemented in digital systems are frequently specified in Laplace transform form. To implement these functions digitally requires a discrete time representation of such functions. For the Space Shuttle Engine Controller Program, this transformation from Laplace to a discrete-time representation is accomplished by the "Tustin" mapping technique, which yields a linear recursion form of the control functions. The "Tustin method" is applied as follows:

Let:  $s$  = Laplace operator or complex frequency variable

$z = e^{sT}$ ; represents advance operator

$d = e^{-sT}$ ; represents delay operator

$T$  = Sampling interval, in seconds

$G(s)$  = An arbitrary transfer function

Given a transfer function  $G(s)$ , one substitutes:

$$s = \frac{2}{T} \frac{(1-d)}{(1+d)} = \frac{2}{T} \frac{(z-1)}{(z+1)}$$

The results are simplified to the form:

$$G(s) \text{ gives } G(d) = \frac{a_0 + a_1(d) + a_2(d)^2 + \dots + a_m(d)^m}{1 - b_1(d) - b_2(d)^2 - \dots - b_m(d)^m}$$

where:  $a_i, b_i$  are the delay coefficients

$m$  is the same for numerator and denominator, and is equal to the degree of the transfer function (highest power of  $s$ ).

The corresponding recursion formula is:

$$Y_n = a_0x_n + a_1x_{n-1} + a_2x_{n-2} + \dots + a_mx_{n-m} \\ + b_1Y_{n-1} + b_2Y_{n-2} + \dots + b_mY_{n-m}$$

where:  $y_n, x_n$  are the output and input value sequences respectively.

$n, n-1, \dots, n-m$  indicate the current value, the previous value, . . . etc respectively.

6.3 The Tustin Method (Continued)

Example 1 : Given the integrator  $G(s) = \frac{1}{s}$ , then

$$G(d) = \frac{1}{2 \frac{1-d}{T} (1+d)} = \frac{T}{2} \frac{(1+d)}{(1-d)}$$

and the recursion form is

$$y_n = \frac{T(x_n + x_{n-1})}{2} + y_{n-1}$$

This is the trapezoidal rule of numerical integration.

Example 2: The following example shows the application of the Tustin method to the transfer function for the MOV illustrated in Figure 10:

$$F(s) = \frac{1/0.16}{s + 1/0.16} = \frac{1}{(0.16)s + 1}$$

$$F(d) = \frac{1}{(0.16) \frac{2}{T} \frac{(1-d)}{(1+d)} + 1} ; T = 0.02 \text{ seconds}$$

$$F(d) = \frac{1}{\frac{16(1-d)}{(1+d)} + 1} = \frac{(1+d)}{16(1-d) + (1+d)}$$

$$F(d) = \frac{(1+d)}{17 - 15(d)} = \frac{1/17 + (1/17)(d)}{1 - (15/17)(d)}$$

The recursive expression is

$$y_n = (1/17)x_n + (1/17)x_{n-1} + (15/17)y_{n-1}$$

6.3 The Tustin Method (Continued)

The recursive expression using the notations of Figure 10 is

$$X_{\text{MOV}} = (1/17) (\text{MOST}) + (1/17) (\text{Prev MOST}) + (15/17) (\text{Prev } X_{\text{MOV}})$$

where:  $X_{\text{MOV}}$  = Current major cycle output to the MOV.

MOST = Current major cycle MOV Start/Shutdown scheduled command.

Prev MOST = Previous major cycle MOV Start/Shutdown scheduled command.

Prev  $X_{\text{MOV}}$  = Previous major cycle output to the MOV.

A simple justification of the Tustin method is sketched in the next paragraph.

A delay of time  $T$  has transfer function  $e^{-sT}$ . One application in filter theory is approximating such delays with lumped-parameter filters, i.e., with rational transfer functions. The best first-order approximation of this delay is:

$$e^{-sT} = \frac{e^{-sT/2}}{e^{+sT/2}} = \frac{1 - sT/2}{1 + sT/2} \quad (\text{approximately})$$

For example, if  $s = j\omega$  (sinusoidal analysis) then

$$e^{-j\omega T} = \frac{1 - j\omega T/2}{1 + j\omega T/2}$$

Converting the equation to polar form (i.e. magnitude / phase angle) gives:

$$1.0 \angle -\omega T = 1.0 \angle -2\arctan(\omega T/2)$$

Thus the right-hand side has the correct magnitude of 1.0 at all frequencies, and the phase angle,  $-2\arctan(\omega T/2)$ , approximates  $-\omega T$  very well for a considerable range of lower frequencies. But if the right-hand side is a good approximation to the left, the converse surely is true.

6.3 The Tustin Method (Continued)

Let  $d = e^{-sT}$  which is approximated by

$$d = \frac{1 - sT/2}{1 + sT/2}$$

then solving the approximate equation for the  $s$  operator, gives

$$s = \frac{2}{T} \frac{(1 - d)}{(1 + d)}$$

The bilinear transformation from the  $s$  operator to  $d$  operator automatically maps stable continuous-time filters (poles in left half of  $s$ -plane) into stable discrete filters (poles outside of the unit circle in the  $d$ -plane, or inside the unit circle in the  $Z$ -plane).

The cascading property holds; e.g., transforming  $1/s^2$  directly, gives identical result as transforming  $1/s$  and  $1/s$  separately and cascading them together. Accuracy by this technique is always reasonable, sometimes very good.

In the process of mapping the left half of the  $s$ -plane to the unit circle, the frequency of the system will be warped. In order to avoid this, the analog system is usually pre-warped before the transformation occurs.

A prewarping analysis of the transformation used in the SSMEC Program was performed, and the results showed that the sampling time was significantly short compared to the response time of the engine. Therefore, prewarping of the Tustin values is not necessary.