SSFF HEALTH MANAGEMENT

ANALYSIS REPORT

PART II (PROOF OF CONCEPT)

DECEMBER 15, 1995

Reference: Contract No. NAS8-40365

Submitted to:
Systems Requirements & Verification Branch
Systems Engineering Division
Systems Analysis and Integration Laboratory
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35801

ALPHA TECHNOLOGY
3322 S. MEMORIAL PARKWAY, SUITE 215H, HUNTSVILLE, AL 35801

SSFF HEALTH MANAGEMENT

ANALYSIS REPORT

PART II (PROOF OF CONCEPT)

DECEMBER 15, 1995

Reference: Contract No. NAS8-40365

Submitted to:
Systems Requirements & Verification Branch
Systems Engineering Division
Systems Analysis and Integration Laboratory
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35801

ALPHA TECHNOLOGY
3322 S. MEMORIAL PARKWAY, SUITE 215H, HUNTSVILLE, AL 35801

THE PART II, PROOF OF CONCEPT, PHASE HAS BEEN SUCCESSFULLY COMPLETED.

ENCLOSED IN THIS REPORT ARE THE FOLLOWING ATTACHMENTS

1) GUIDELINES AND ASSUMPTIONS

2) SUMMARY/CONCLUSIONS

3) FF-DAREL WORKSHEETS WITH SUPPORTING ENCLOSURES

   - GDS SCHEMATIC
   - FUNCTIONAL BLOCK DIAGRAM
   - GDS MECHANICAL/ELECTRICAL I/F
   - BLOCK FUNCTIONS TABLE
   - FUNCTIONAL FAILURES TABLE
   - ACTIVE COMPONENTS IN FUNCTIONAL BLOCKS

4) MAINTAINABILITY AND RELIABILITY CONSIDERATIONS IN HEALTH MANAGEMENT

1. GUIDELINES/ASSUMPTIONS

* Evaluate/Analyze only the Gas Distribution Subsystem (GDS)

* Focus HM activities on the FF-DAREL Process

* Use the PDR Configuration (per COTR instruction)

(All are aware that this configuration has change considerably since PDR)

* Develop HM Requirements from all available data on all subsystems. (This is more mature information than would normally be available for use in defining requirements). Make assumptions, as necessary to complete this effort.

* If a "Component" fails in our analysis, we do not concern ourselves as to how it fails, except to the extent of all the "Resulting Effects"

2. SUMMARY/CONCLUSIONS

The Gas Distribution Subsystem was studied and evaluated utilizing the PDR Configuration and with respect to the design features encompassing Health Management (HM) aspects outlined in the Generic Handbook (specifically the FF-DAREL Process). This HM effort addresses equipment and failures at a higher level than FMEA efforts and results in less worksheets, and focuses results toward "Test" and "Operations" issues.

We were only able to conduct limited discussions with the skilled designers who are extremely knowledgeable of the GDS. This limitation has probably resulted in somewhat shallow analysis, but, the major subjects have been addressed and evaluated.

The GDS is largely a self contained subsystem, and is largely simplex, but some redundancy is included in the design and its functions have been identified and its use in HM have been analyzed. The lack of needed, or possibly desired, redundancy is also identified and its impact is assessed. A significant lack of "two fault tolerant Functional Failure" cases (component and paths) are identified and a recommendation for simple inclusion of redundancy is being discussed with the Detail Designer. The details of the approach could be pursued, if desired, by the Detail Design Engineer. A significant amount of manual operations to perform "Corrective Action" has been identified (even operational procedures). This condition often precludes utilizing software to isolate and recover from Functional Failures.

The software is not yet mature and detail was not available to us to insure whether or not Paragraph 3.1.2.6.3.1 in the S/W Requirement Specification, Level III (The S/W shall be capable of detecting, isolating, and responding to faults within the GDS) is being met. Our conclusion is that the PDR GDS configuration will not allow this requirement to be accommodated in many instances (identified in the FF-DAREL Worksheets). Accommodating this requirement is a significant effort, but is vital to our HM Concept and would be documented in the ISIRL for each Functional Failure and for use in Test and Operations. Note: The S/W requirement is also stated in the "Core System Requirement Document", Para. 3.3.7.

The results of this study have shown a definite need for coordinating need for measurements within, and between, subsystems to accommodate insuring that Functional Failures are properly revealed and can be substantiated as valid by other measurements, even from other interfacing subsystems.

We were not able to perform a major goal of our Concept involving "Developing an additional level of Information by defining Intersystem Informational Relationships". This was because the Experiment Module (EM) and ICE are the only electrical interfaces to the GDS. The EM (specifically, the Crystal Growth Module) has just within the past few days identified a significant number of measurements for that system. This will allow some additional HM considerations and evaluations, but time was not available to perform this task. The ICE Interface is more mature, but was not addressed because of guidelines and time constraints on this effort. These efforts can be readily accomplished with additional time to perform the assessments.

We have concluded that the HM aspects in our Concept could have been significantly enhanced in the GDS design had the Concept been in place at the start of the Initial Design Phase of the Project. However, we feel that this Part II, Proof of Concept Phase, has been very successful and has accomplished its purpose and indicates very useful types of information which can be gleaned and evaluated from the current design and useful to the Project and Project Manager in upcoming Reviews and throughout the SSFF Development/Operational Phase.

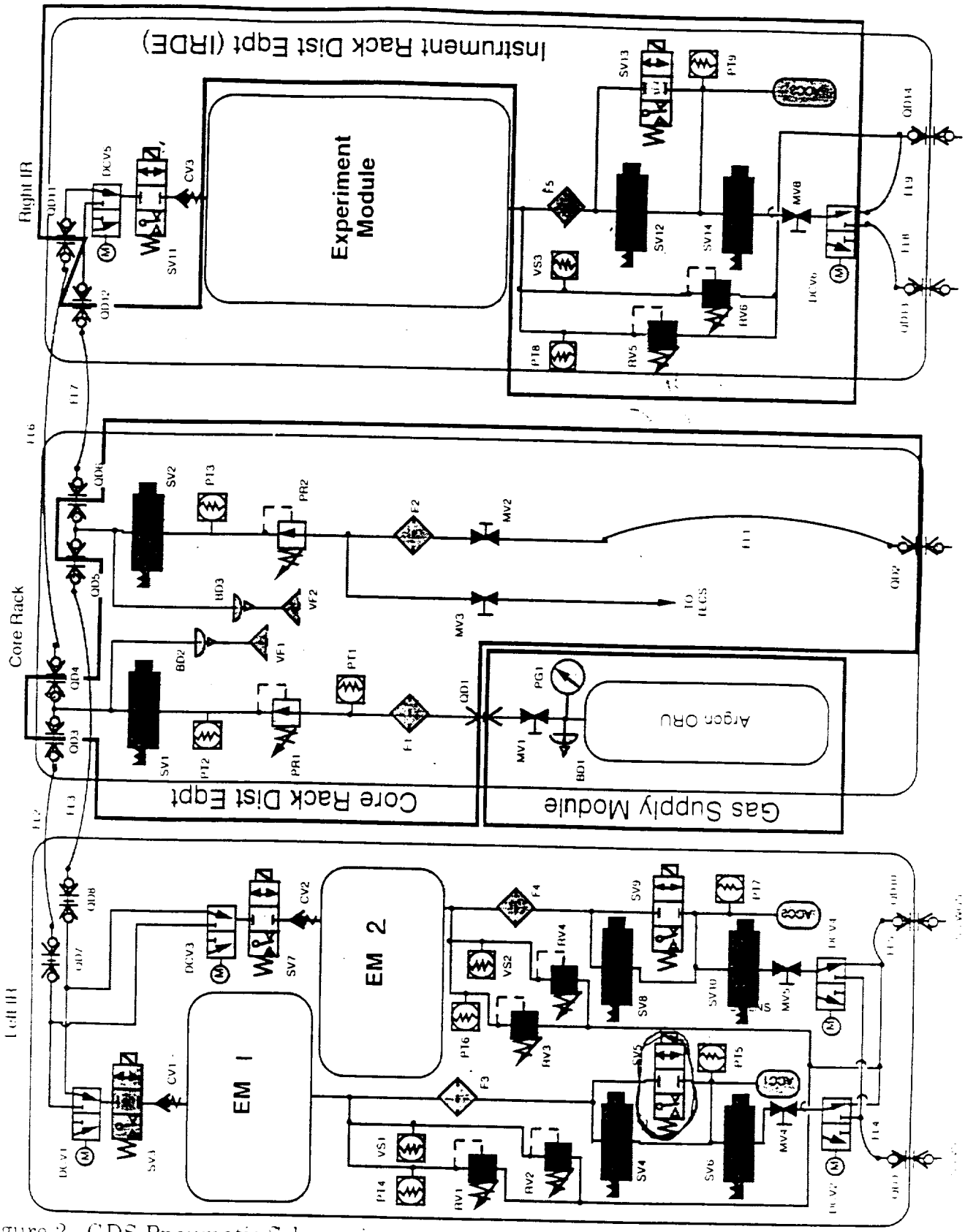
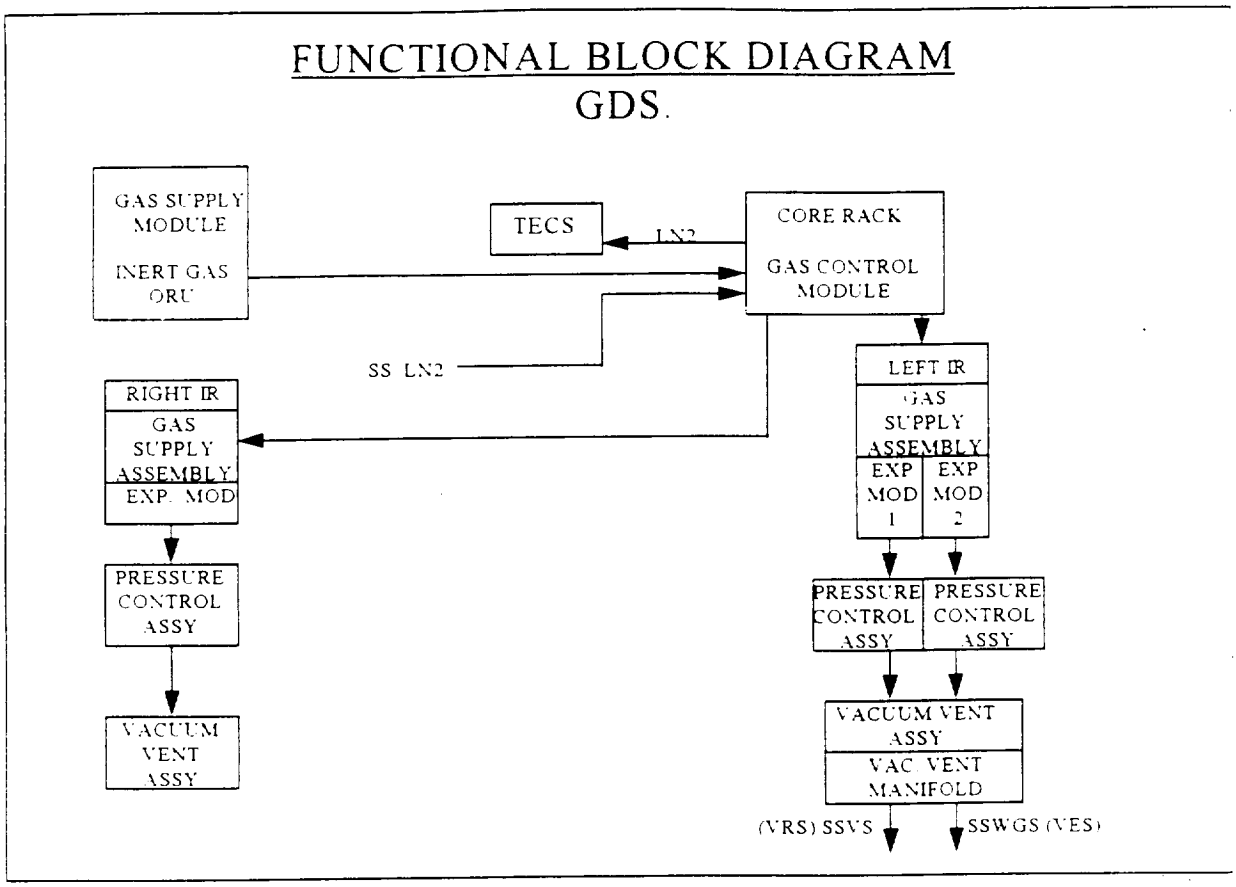
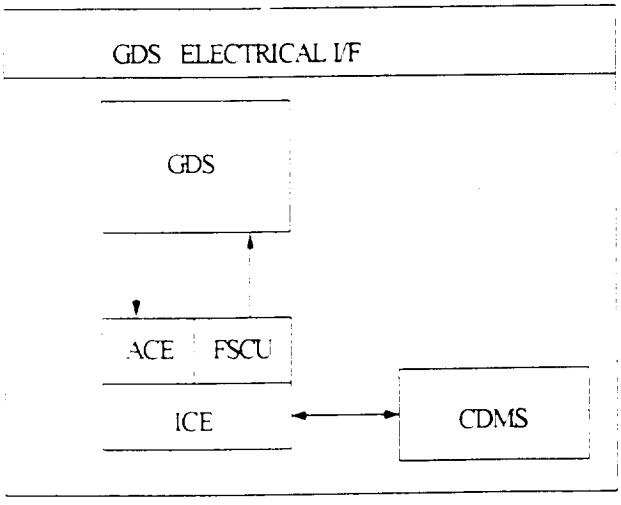
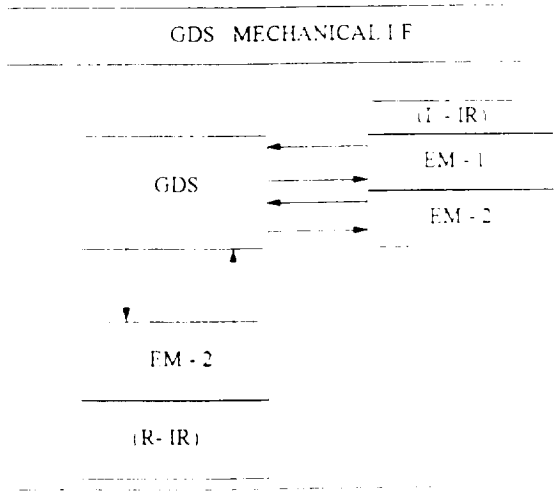


Figure 2. GDS Pneumatic Schematic

3. FF-WORKSHEETS WITH SUPPORTING ENCLOSURES







BLOCK FUNCTIONS TABLE

1. GAS SUPPLY MODULE
   a. Supplies inert gas to Core Rack gas control module when manual valve is open
   b. Provides safety over pressure device (BD1)
   c. Provides manual pressure readout at all times

2. CORE RACK GAS CONTROL MODULE
   a. Provides control (manual valve) and filtering of GN2 from SSLNS to TECS
   b. Provides filtering pressure regulation and control (SV) of LN2 to IR (Left & Right) gas supply assemblies
   c. Provides filtering, pressure regulaton and control (SV) of (AR) to IR (Left & Right) gas supply assemblies
   d. Provide over pressure safety devices (BD2,BD3)

3. GAS SUPPLY ASSEMBLY (2 EACH, 1 OF WHICH HAS 2 SEPARATE,DUAL FUNCTIONS)
   a. Provides source gas (AR or LN2) selection
   b. Provides (Selected) gas control (SV) to EM
   c. Provide blocking of EM gasses which might travel backward to GDS (CV)

4. PRESSURE CONTROL ASSEMBLY (3 EACH, 1 FOR EACH EM)
   a. Provides control (SV) of EM gasses to accumulator (for use when SS Vacuum Exhaust System is not available)

5. VACUUM VENT ASSEMBLY (2 EACH, 1 OF WHICH SERVES 2 EM'S)
   a. Provides particle filtering
   b. Provides pressure relief (RV) [2 relief (redundant) valves for each EM]
      -- To Vacuum Exhaust System
   c. Provides Control (2 series SV & MV & DCV) of exhaust gasses to VES
   d. Provides Control (SV &MV) drainage of accumulator to VES
   e. Provides Selection of VRS or VES to downstream (outlet side) of EM

FUNCTIONAL FAILURES

1 GAS SUPPLY MODULE

a Fails to supply inert gas to core rack gas control

b Fails to stop supplying inert gas to core rack

c Failure to provide over pressure relief

d Manual pressure gage fails to provide readout

2 CORE RACK GAS CONTROL MODULE

a Fails to provide control and filtered LN2 to TECS

b LN2 to IR (Left and/or Right) gas supply assemblies

- Fails to filter
- Fails to provide proper regulation
- Fails to supply

c AR to IR (Left and/or Right) gas supply assemblies

- Fails to filter
- Fails to provide proper regulation
- Fails to supply

d Fails to provide over pressure relief

3 GAS SUPPLY ASSEMBLY

a DCV 1, 3 or 5 fails to allow selection of source gas

b SV3, 7 OR 11 fails to control (On/Off) gas flow to EM

c CV1, 2 OR 3 fails to block EM gasses backflow into GDS

4 PRESSURE CONTROL ASSEMBLY

Fails to vent EM gasses to accumulator when commanded

5 VACUUM VENT ASSEMBLY

a Fails to provide particle filtering

b Fails to provide EM pressure relief to VES (Redundant)

Fails to provide EM pressure relief to VES (Redundant)

c SV4, 8, 12 fails to vent EM exhaust gasses to VES when commanded

d SV6, 10, 14 and MV4, 5 & 6 fails to provide drainage of accumulator to VES when commanded

e DCV2, 4, 6 fails to select VRS or VES to down stream EM when commanded

ACTIVE COMPONENTS IN FUNCTIONAL BLOCKS

I GAS SUPPLY MODULE

- Pressure Vessel	PV1
- Pressure Gauge	PG1
- Safety Device	BD1
- Manual Valve	MV1
- Quick Disconnect	QD1

II CORE RACK GAS CONTROL MODULE

For LN2

- Quick Disconnect	QD4
- Manual Valve	MV2
- Filter (01Mic)	F2
- Manual Valve	MV3
- Pressure Regulator (1 Stage)	PR2
- Pressure Transducer	PT3
- Solenoid Valve	SV2
- Burst Disc	BD3
- Vent Filter	VF2
- Quick Disconnect	QD5
- Quick Disconnect	QD6

For Inert (AR) Gas

- Filter (01 Mic)	F1
- Pressure Transducer	PT1
- Pressure Regulater	PR1
- Pressure Transducer	PT2
- Solenoid Valve	SV1
- Burst Disc	BD2
- Vent Filter	VF1
- Quick Disconnect	QD2
- Quick Disconnect	QD3

III GAS SUPPLY ASSEMBLY (RIGHT IR)

- Quick Disconnect (AR)	QD11
- Quick Disconnect (LN2)	QD12
- Directional Control Valve	DCV5
- Solenoid Valve	SV11
- Check Valve	CV3
- Experiment Module	EM(R-IR)

IV PRESSURE CONTROL ASSEMBLY (RIGHT IR)

- Pressure Transducer	PT8
- Vacuum Sensor	VS3
- Solenoid Valve	SV13
- Pressure Transducer	PT9
- Accumulator	ACC3

V VACUUM VENT ASSEMBLY (RIGHT IR)

- Relief Valve	RV5
- Relief Valve	RV6
- Filter (01Mic)	F5
- Solenoid Valve	SV12
- Solenoid Valve	SV14
- Manual Valve	MV6
- Directional Control Valve	DCV6
- Quick Disconnect (VRS)	QD13
- Quick Disconnect (VES)	QD14

VI GAS SUPPLY ASSEMBLY (LEFT IR)

- Quick Disconnect (AR)	QD7
- Quick Disconnect (GN2)	QD8

For EM-1

- Directional Control Valve	DCV1
- Solenoid Valve	SV3
- Check Valve	CV1
- Experiment Module	EM-1

For EM-2

- Directional Control Valve	DCV3
- Solenoid Valve	SV7
- Check Valve	CV2
- Experiment Module	EM-2

VII PRESSURE CONTROL ASSEMBLY (LEFT IR)

For EM-1

- Pressure Transducer	PT4
- Vacuum Sensor	VS1
- Solenoid Valve	SV5
- Pressure Transducer	PT5
- Accumulator	ACC1

For EM-2

-Pressure Transducer	PT6
- Vacuum Sensor	VS2
- Solenoid Valve	SV9
- Pressure Transducer	PT7
- Accumulator	ACC2

VIII VACUUM VENT ASSEMBLY (LEFT IR)

- Quick Disconnect (VRS)	QD9
- Quick Disconnect (VES)	QD10

For EM-1

- Relief Valve	RV1
- Relief Valve	RV2
- Filter (01Mic)	F3
- Solenoid Valve	SV4
- Solenoid Valve	SV6
- Manual Valve	MV4
- Directional Control Valve	DCV2

For EM-2

- Relief Valve	RV3
- Relief Valve	RV4
- Filter (01Mic)	F4
- Solenoid Valve	SV8
- Solenoid Valve	SV10
- Manual Valve	MV5
- Directional Control Valve	DCV4

4. MAINTAINABILITY AND RELIABILITY CONSIDERATIONS IN HEALTH MANAGEMENT

4.1 INTRODUCTION

The Space Station Furnace Facility (SSFF) is a modular facility which will provide the platform for materials research in the microgravity environment. The facility is designed to accommodate Experiment Modules (EM) which house an experiment. The facility will provide the function of interfacing the EM to ISSA services, conditioning and control for the experiment module use, providing the controlled services to the experiment modules, and interfacing to and acquiring data from the experiment modules.

The SSFF has several subsystems which provide the above mentioned functions. The Subsystems are Electrical Power Subsystem (EPS), Command and Data Management Subsystem (CDMS), Gas Distribution Subsystem (GDS), Thermal and Environmental Control Subsystem (TECS), and the Instrumentation and Control Electronics (ICE) Subsystem.

4.2 HEALTH MANAGEMENT INTRODUCTION

The facility is designed, constructed, tested to determine to be in an operable state, and lifted into space. Once in orbit, the SSFF is available to be placed on-line and to accept EM's in order to perform experiments. The EMs are to be removed and replaced as required and remain in operation for 2880 hours. This means that the SSFF is a mission oriented system. Analysis will determine whether the system is to be a repairable or non-repairable system.

4.3 SYSTEM LEVEL HEALTH MANAGEMENT ANALYSIS

For the SSFF to accomplish its intended purpose, it must operate without failure for 2880 hours. Since reality states that perfection is impossible, trade-offs must be made so that the mission can be accomplished in a cost effective manner. The intent is to minimize the cost and successfully accomplish the intended mission. For example, say that the cost of an EM plus the cost of lifting the EM into orbit is $600,000.00 and each EM can be used only once. Table 1 shows an assumed relationship between Cost and P(MS). Assume that the allowable budget is $2.4 million. This means that the P(MS) must be 0.97 in order to meet budget in order to have a guaranteed successful mission. But, trade studies reveals that it is possible to build a system that meets a P(MS) or reliability of 0.94; however, that it is very costly to build an SSFF that meets a reliability of 0.97. Thus engineering must perform some trade-offs in order that a successful mission can be performed as well as to be within cost.

It is known that the SSFF is composed of five subsystems. A network model of the subsystems is a series system. This means that all of the subsystems must work for the system to be a success. If one subsystem fails, then the system fails. Figure 1 shows the network model. Equation 1 is the mathematical expression that represents the network model.

P(MS)	cost to achieve success (worst case)
0.99	1.2
0.98	1.8
0.97	2.4
0.96	3.0
0.95	3.6
0.94	4.2

TABLE 1 COST Vs P(MS)

$$P(MS) = P(EPS) * P(TECS) * P(CDMS) * P(ICE) * P(GDS) \quad (1)$$

Where: P(MS) is the probability of mission success

P(EPS) is the probability that the EPS does not fail

P(TECS) is the probability that the TECS does not fail

P(CDMS) is the probability that the CDMS does not fail

P(ICE) is the probability that the ICE does not fail

P(GDS) is the probability that the GDS does not fail

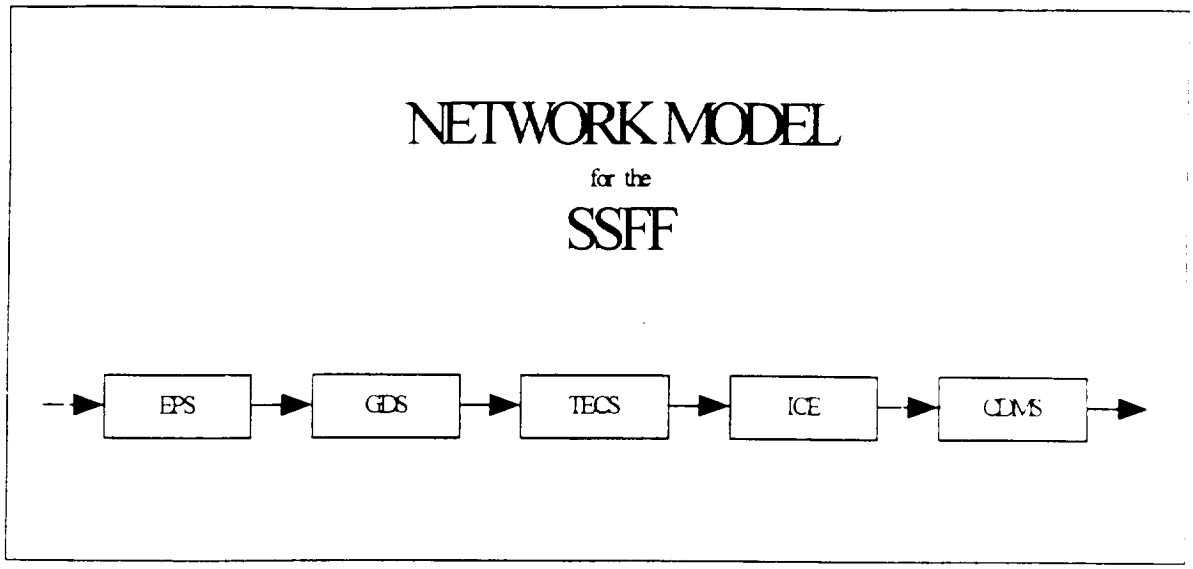


Figure 1 Network Model of the SSFF

First some approximate values of the probability of mission success will be selected. From Table 1, a value for P(MS) of 0.94 seems to be a practical selection for a beginning analysis. Since a P(MS) has been selected, the determination of test criteria can be investigated.

P(MS) (PROBABILITY OF MISSION SUCCESS)	P(SS) (PROBABILITY OF SUBSYSTEM SUCCESS)
0.99	0.99799
0.98	0.99596
0.97	0.99393
0.96	0.99187
0.95	0.98979
0.94	0.98770

Table 2, Trial P(MS)

Consider the SSFF as a single component system having a time-to-failure that is exponentially distributed. Evaluate analytically and by simulation the model using a P(MS) of 0.94 for a period of 2880 hours. Equation 2 is used to determine a trial failure rate for the SSFF

$$P(MS) = \exp(-\lambda t) \qquad (2)$$

$$0.94 = \exp(-\lambda * 2880)$$

$$\lambda = \text{Ln}(0.94)/2880$$

$$\lambda = 0.2148/10 \text{ exp } 6 \text{ f per hr} \quad (3)$$

Equation 3 is the failure rate at which the SSFF must operate in order to provide the P(MS) of 0.94. This failure rate must be distributed over the five subsystems. From Equation 1.0, assuming that all subsystem failure rates are equal, the P(MS) equals to 0.9877.

This means that the failure rate for each subsystem is,

$$\lambda = 4.297/10 \text{ exp } 6 \text{ f per hr} \quad (4)$$

Hence, the next step is to perform some trade studies to determine the availability of component parts with the required failure rates, cost, and lead time for the procurement of these parts. From experience, the availability of component that possess the required failure rates and meets cost constraints is not cost effective. Trade off's will have to be made.

For this example, the GDS is selected. When perusing the SSFF Maintainability Analysis, a component in GDS was found that had a high failure rate of 21.9 failures for every million hours. When evaluating the P(MS) of the subsystem and entire SSFF, this high failure rate component was found to be a series element in the network model. The P(MS) of this component is 0.9389. This figure is lower than the system P(MS).

In Section 2 above, it was stated that the determination of the system type as to a repairable or non-repairable system would be made. From the results of the trade studies mentioned in the previous paragraph, the system must be a repairable system in order to meet the P(MS) of 0.94. By using maintainability, the system P(MS) can be raised in a very cost effective manner. It is universally agreed that component parts with lower and lower failure rates are expensive and a high man-hour requirement for maintenance is also very expensive. Again a trade study is needed to determine a cost effective balance. Let's say that the trade study revealed that no science will be lost if this high failure part can be replaced and the system returned to operation within 30 minutes. This decision will accomplish two things, the P(MS) of the system will be increased and the cost will be reduced. Secondly, by managing the failure rate of the component, the requirement for low failure components is reduced.

Let's investigate the test requirements for this maintenance action. From Equation 5, the relative uncertainty can be calculated. From this analysis, test criteria will be selected. It is given that the average time to repair the part or MTTR is 30 minutes. Assume a standard deviations of 1or 3 minutes. How many trial runs are needed to yield certainty of success. Using Equation 5, Table 2 was constructed. The Table shows that as the number of trials increase the degree of uncertainty decreases. Also as the standard deviation decreases or narrows, the number of

required trials increases for a desired level of certainty. From Table 2, the selection of a certainty is selected with a standard deviation of one. The reason for the selection is for a fewer number of trials the higher degree of certainty is achieved.

$$R_{un} = S / X\sqrt{n} \qquad (5)$$

Where R_{un} = Relative Uncertainty of the Trial Test

S = Standard Deviation

X = Average or Mean Value

n = Number of Trials Required

n	S	X	Unc	C
1	3	30	0.1	0.90
4	3	30	0.05	0.95
25	3	30	0.02	0.98
36	3	30	0.016	0.983
1	1	30	0.033	0.97
4	1	30	0.017	0.98
25	1	30	0.007	0.99
36	1	30	0.006	0.99

Table 2. Relationship between Number of Test Trials Vs Degree of Certainty

4.4 REQUIREMENTS

The HM requirements of the GDS can be stated.

The failure rate of the following systems shall be no greater than 4 297 failures in one million hours.

1. EPS
2. TECS
3. ICE
4. CDMS

The GDS shall have a mean time to repair (MTTR) of 30 minutes with a standard deviation of 3 minutes.

Test requirements shall be that sufficient trials be conducted so that a 98% degree of certainty is achieved. The number of trials shall not be less than 25. The success criteria shall be that 98% of the trials result in the replacement of the single component and the SSFF returned to service in less than or equal 30 minutes.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY MODULE
DRAWING SCHEMATIC
REF DES

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 1 a PAGE 1
DATE 12 - 10 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
1 a	1 a	1) ARGON TANK RUPTURE 2) ARGON TANK LEAK 3) MANUAL VALVE (MV1) FAILS TO OPEN 4) BURST DISK RUPTURE/LEAK	- NO INET GAS FOR HIGH TEMP FURNACE OPERATION	1 SEC (PT1 = 1 S/S)	ACTIVATING THIS SEGMENT OF GAS SUPPLY IS A MANUAL PROCEDURE- REMAINING ACTIVATION STEPS COULD BE HELD UP INDEFINITELY, PENDING CORRECTIVE ACTION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FFNO 1 a PAGE 2

DATE 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
NO	1) ORU AR TANK (MANUAL PROCEDURE) 2) ORU AR TANK (MANUAL PROCEDURE) 3) T/S VALVE (MANUAL PROCEDURE) 4) T/S- REPLACE BURST DISK	NONE	PG-1, PT-1 (PRIME) PP-2 (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE.
NOT TIME CRITICAL - NO S/W DETECTION, ISOLATION, RECOVRY REQ'D.
- A MANUAL PROCEDURE OPERATION.

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN.
NO REQUIREMENT TO SIMULATE FAILURE IN SIM LAB/TEST BED.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY MODULE
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
__ PRE-LAUNCH
__ ASCENT
__ DEPLOYMENT
X OPERATIONS
__ CONTINGENCY/RETURN

FF NO: 1.b PAGE 1

DATE: 12 - 10 - 95

(1) FF NO	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
1 b	1 a	MANUAL VALVE (MV1) IN OPERATIVE	NO FUNCTIONAL EFFECT - CAN BE CONTROLLED BY SV1 (CONTROLS AR TO LEFT AND RIGHT IR RACKS)	1 SECOND (PT1 & SV1 WOULD INDICATE FAILURE - ASSUMING ICE AND CDMS ARE OPERATING	THIS IS PART OF A MANUAL PROCEDURE CAN WORK AROUND PROBLEM WITH COMMAND TO SV1

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 1b PAGE 2

DATE, 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
NO	T/S MANUAL VALVE (MV1) (MANUAL PROCEDURE)	NONE	PT-1 (PRIME) PT-2 (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
NOT TIME CRITICAL - NO S/W DETECTION, ISOLATION, RECOVERY REQUIRED
- A MANUAL PROCEDURE OPERATION

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN
NO REQUIREMENT TO SIMULATE FAILURE IN SIM LAB/TEST BED

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY MODULE
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE _____PRE-LAUNCH
_____ASCENT
_____DEPLOYMENT
X OPERATIONS
_____CONTINGENCY/RETURN

FF NO 1 c

PAGE 1

DATE 12 - 10 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
1 c	1 b	DISK FAILS TO RUPTURE UPON OVER PRESSURE	POSSIBLE TANK RUPTURE - (NO KNOWN CAUSE FOR OVER PRESSURE. BUT, THE RELIEF MECHANISM IS PROVIDED)	1 SEC (PT1 = 1 S/S) IF ICE - CDMS ARE OPERATING OR - IF PG1 IS BEING OBSERVED - (3200 PSI BURST POINT)	IMMEDIATE

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 1 c PAGE 2

DATE, 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
YES	NONE PRESENTLY COULD OCCUR - RESPONSE MUST BE IMMEDIATE (AGAIN - NO CAUSE FOR OVER PRESSURE IS KNOWN)	NONE	PG-1 (PRIME) PT-1 (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
TIME CRITICAL - ANY CORRECTION ACTION MUST BE BY S/W LOGIC/ACTION.

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN
SHOULD LOOK AT S/W DETECTION/RESPONSE - AND CONSIDER SIM LAB/TEST BED SIMULATION

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF MISSION PHASE: PRE-LAUNCH FF NO: 1 d PAGE 1
SUBSYSTEM/ASSY GDS ASCENT
COMPONENT/EQUIP GAS SUPPLY MODULE DEPLOYMENT DATE: 12 - 10 - 95
DRAWING SCHEMATIC -- X OPERATIONS
REF DES: -- CONTINGENCY/RETURN

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
1 d	1 c	MALFUNCTIONING PRESSURE GAGE	NO FUNCTIONAL EFFECT - (A MANUALLY READ PRESSURE GAGE) - NO ICE I/F.	IMMEDIATE (UPON OBSERVATION)	REPLACE WITH ORU AR TANK (WHEN NORMALLY ACCOMPLISHED)

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO: 1 d PAGE 2

DATE: 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
NO	REPLACE WHEN AR TANK IS REPLACED	NONE - BUT (PT1 CAN PROVIDE INFORMATION NEEDED)	PT-1 (PRIME) PT-2 (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
NOT TIME CRITICAL - NO S/W DETECTION, ISOLATION, RECOVERY REQ'D
- A MANUALLY READ GAGE/MEASURMENT

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN - NONE REQUIRED NO REQUIREMENT TO SIMULATE FAILURE IN SIM LAB/TEST BED

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF MISSION PHASE _____PRE-LAUNCH FF NO. 2 a PAGE 1
SUBSYSTEM/ASSY GDS _____ASCENT
COMPONENT/EQUIP CORE RACK GAS CONTROL MODULE _____DEPLOYMENT DATE 12 - 10 - 95
DRAWING SCHEMATIC -- X_____OPERATIONS
REF DES -- _____CONTINGENCY/RETURN

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
2 a	2 a	1) MV2 FAILS TO OPEN 2) F2 CLOGS 3) MV3 FAILS TO OPEN	TECS ACCUMULATOR WILL NOT BE ABLE TO BE PRESSURIZED WITH GN2 (SEE "NOTE 1")	1 SEC (MEAS NO USZTEP) (ACCUM PRESS) SAMPLE RATE = 1 S/S - IF ICE - CDMS IS OPERATIONAL	TBD - (INVOLVES TECS OPERATIONS)

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE
"NOTE 1" - FAILURE CAUSES 2) & 3) ALSO RESULT FROM "FUNCTIONAL FAILURE" 2 b

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 2 a PAGE 2

DATE 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
NO	T/S MV2 (MANUAL PROC) T/S F2 (MANUAL PROC) T/S MV3 (MANUAL PROC)	NONE	USZTEC (PRIME) (TBD -TEC) (BACK UP) PT3 (FOR MV2 AND F2 CAUSES)(BACK-UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE.
NOT TIME CRITICAL - NO S/W DETECTION, ISOLATION, RECOVERY REQUIRED.
(ALL MANUAL OPERATIONS)

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN - NO REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP CORE RACK GAS CONTROL MODULE
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
_____PRE-LAUNCH
_____ASCENT
_____DEPLOYMENT
X OPERATIONS
_____CONTINGENCY/RETURN

FF NO 2 b PAGE 1
DATE 12 - 10 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
2 b	2 b	1) F2 CLOGS 2) PR2 FAILS TO REGULATE 3) SV2 FAILS TO OPERATE	1) LOSS OF LN2 TO TECS - (SEE FF NO. 2.a) 2) LOSS OF REGULATED LN2 TO EM EXPERIMENT MODULES 3) LOSS OF CONTROL OF GN2 FLOW TO EXPERIMENT MODULES	1 SEC (PT3) IF ACC/CDMS ARE OPERATIONAL (FOR F2 AND PR2 CAUSES) - SV2 FAILURE INDICATION TIME DEPENDS ON EXP. MOD DATA (NOT YET AVAILABLE)	TBD - PENDING EM OPERATIONS AND TECS OPERATIONS IF F2 COLGS

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO: 2 b PAGE 2

DATE: 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
(POSSIBLE) PENDING ADDITION-AL ANALYSIS OF EM & TECS OPER-ATIONS	PENDING ADDITIONAL ANALYSIS : T/S F2 (MANUAL PROC) T/S PR2 (MANUAL PROC) T/S SV2 (MANUAL PROC)	NONE	F2 CLOGS & PR2 FAILS TO REGULATE : PT3 (PRIME) TBD (EM FURNACE) (BACK-UP) SV2 FAILURE TO OPERATE : SOLELY DEPENDENT ON EM (FURNACE) MEASUREMENTS (TBD)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
TIME CRITICALITY NEEDS MORE ANALYSIS S/W DETECTION, ISOLATION, RECOVERY NEED IS PENDING

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED PENDING

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP CORE RACK GAS CONTROL MODULE
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE:
_____PRE-LAUNCH
_____ASCENT
_____DEPLOYMENT
X_____OPERATIONS
_____CONTINGENCY/RETURN

FF NO 2.c PAGE 1
DATE 12 - 10 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
2 c	2 c	1) F1 CLOGS 2) PR1 FAILS TO REGULATE 3) SV1 FAILS TO OPERATE	1) & 2) LOSS OF REGULATED AR GAS TO EM EXPERIMENT MODULES 3) LOSS OF CONTROL OF AR GAS FLOW TO EXPERIMENT MODULES	1 SEC (PT2 = 1 S/S) IF ACC/CDMS IS OPERATING. FOR F1 CLOG AND PRESSURE REGULATOR FAILURE - TBD FOR SV1 FAILURE (DEPENDS ON MEASUREMENTS IN EM FURNACE)	TBD - PENDING ADDITIONAL ANALYSIS ON EM FURNACE OPERATIONS

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 2 c PAGE 2

DATE. 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
(POSSIBLE) PENDING ADDITION-AL ANALYSIS OF EM OPER-ATIONS	PENDING ADDITIONAL ANALYSIS T/S F1(MANUAL PROC) T/S PR2 (MANUAL PROC) T/S SV2 (MANUAL PROC)	NONE	FOR F1 CLOGS & PR1 FAILS TO REGULATE PT2 (PRIME) TBD (EM FURNACE MEAS) (BACK-UP) FOR SV1 FAILURE : SOLELY DEPENDENT ON EM FURNACE MEASUREMENTS (NOT YET AVAILABLE)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
TIME CRITICALITY NEEDS MORE ANALYSIS NEED FOR S/W DETECTION, ISOLATION, RECOVERY IS PENDING

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP CORE RACK GAS CONTROL MODULE
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
___ PRE-LAUNCH
___ ASCENT
___ DEPLOYMENT
X OPERATIONS
___ CONTINGENCY/RETURN

FF NO 2 d
PAGE 1
DATE 12 - 10 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
2 d	2 d	- BD2 FAILS TO RUPTURE UPON OVER PRESSURE - BD3 FAILS TO RUPTURE UPON OVER PRESSURE	EXCESSIVE EM PRESSURE (POSSIBLE DAMAGE TO FURNACE) NOTE: (ADDITIONAL ANALYSIS ON EM FURNACE REQ'D)	1 SEC (PT2/PT3 – 1 S/S) IF ACC/CDMS IS OPERATIONAL	IMMEDIATE

(1) SEE FUNCTIONAL FAILURES TABLE
(2) SEE BLOCK FUNCTIONS TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 2 d PAGE 2

DATE 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
YES	1) IF BD2 FAILS, SET DCV1, 3, OR 5 TO AR SOURCE AND OPEN SV3, 7, OR 11 ALLOWING AR TO PASS THRU EM TO RELIEF VALVES ON EM EXHAUST SIDE 2) IF BD3 FAILS, SET DCV1, 3, OR 5 TO LN2 SOURCE AND OPEN SV3, 7, OR 11 ALLOWING LN2 TO PASS THRU EM TO RELIEF VALVES ON EM EXHAUST SIDE	NONE	BD2 FAIL PT2 (PRIME) TBD (EM FURNACE) (BACK UP) BD3 FAIL PT3 (PRIME) TBD (EM FURNACE) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE.
TIME CRITICAL (PENDING ADDITIONAL EM ANALYSIS) - ANY CORRECTIVE ACTION MUST BE BY S/W LOGIC/ACTION.

CONCLUSION: NO REDUNDANT COMPONENTS/PATHS IN DESIGN. SHOULD LOOK AT S/W DETECTION/RESPONSE, AND CONSIDER SIM LAB/TEST BED SIMULATION OF FAILURE.

WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY ASSEMBLY
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE: ____PRE-LAUNCH
____ASCENT
____DEPLOYMENT
X____OPERATIONS
____CONTINGENCY/RETURN

FF NO 3 a

PAGE 1

DATE 12 - 11 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
3 a	3 a	1) DCV(X) FAILS TO "OPEN/CLOSE" THRU PATH WHEN COMMANDED	1) LOSS OF LN2 OR AR TO EM FURNACE	1) 1 SEC : 1 S/S DISCRETE	TBD - INVOLVES EM FURNACE OPERATION NOTE : SV3, 7, OR 11 WOULD PREVENT UNWANTED GAS FROM ENTERING EM WHEN DCV FAILURE WAS INDICATED BY MEASUREMENT

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 3 a PAGE 2

DATE, 12-11-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	PENDING EM FURNACE ANALYSIS, AND NEED FOR S/W DETECTION/CONTROL T/S DCV(X) (MANUAL PROCEDURE)	NONE	DCV(X) OPEN/CLOSED DISCRETE (PRIME) TBD (EM FRUNACE) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO): NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE. TIME CRITICALITY NEEDS MORE ANALYSIS. NEED FOR S/W DETECTION, ISOLATION, RECOVERY IS PENDING.

CONCLUSION: NO REDUNDANT COMPONENTS/PATHS IN DESIGN. REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY ASSEMBLY
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
_____PRE-LAUNCH
_____ASCENT
_____DEPLOYMENT
X_____OPERATIONS
_____CONTINGENCY/RETURN

FF NO 3 b
DATE 12 - 11 - 95
PAGE 1

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR. ACTION
3 b	3 b	SV(X) FAILS TO OPERATE	LOSS OF LN2 OR AR TO EM FURNACE	1 SEC : 1 S/S DISCRETE	TBD - INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 3 b PAGE 2

DATE 12-11-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	PENDING EM FURNACE ANALYSIS, AND NEED FOR S/W DETECTION/CONTROL T/S SV(X) (MANUAL PROCEDURE)	NONE	SV(X) OPEN/CLOSED DISCRETE (PRIME) TBD (EM FRUNACE) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE.
TIME CRITICALITY NEEDS MORE ANALYSIS. NEED FOR S/W DETECTION, ISOLATION, AND RECOVERY IS PENDING

CONCLUSION: NO REDUNDANT COMPONENTS/PATHS IN DESIGN. REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP GAS SUPPLY ASSEMBLY
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 3 c
DATE 12 - 11 - 95
PAGE 1

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
3 c	3 c	CV(X) FAILS TO BLOCK EM GAS BACK FLOW TO GDS OR FAILS TO ALLOW INERT GAS TO EM	a CONTAMINATION OF LN2/AR SUPPLY b LOSS OF LN2 (OR AR) TO EM	TBD (PENDING ANALYSIS OF EM FURNACE MEASUREMENTS	TBD - INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 3 c PAGE 2

DATE 12-11-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	PENDING EM FURNACE ANALYSIS, AND NEED FOR S/W DETECTION/CONTROL T/S CV(X) (MANUAL PROCEDURE)	NONE	CV(X) TBD (EM FURNACE MEASUREMENTS) (PRIME AND BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO). NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE. TIME CRITICALITY NEEDS MORE ANALYSIS. NEED FOR S/W DETECTION, ISOLATION, AND RECOVERY IS PENDING. NO AVAILABLE DATA ON MEASUREMENTS INDICATING CV(X) FAILURE.

CONCLUSION. NO REDUNDANT COMPONENTS/PATHS IN DESIGN. REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF MISSION PHASE _____PRE-LAUNCH FF NO 4 a PAGE 1
SUBSYSTEM/ASSY GDS _____ASCENT
COMPONENT/EQUIP PRESSURE CONTROL ASSEMBLY _____DEPLOYMENT DATE 12 - 10 - 95
DRAWING SCHEMATIC -- X_____OPERATIONS
REF DES -- _____CONTINGENCY/RETURN

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
4 a	4 a	SV 5, 9, OR 13 FAILS TO OPERATE	EM MODULE WILL NOT HAVE PROPER GAS FLOW OR VENTING CAPABILITY WHICH COULD POSSIBLY RESULT IN LOSS OF EXPERIMENT	1 SEC 1 S/S DISCRETE	TBD - INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO. 4 a PAGE 2

DATE. 12-10-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
YES	S/W LOGIC AND CONTROL - UPON PREDETERMINED CAVITY PRESSURE/VACUUM VALUES AND FAILURE INDICATION OF SV5, 9, OR 13, ISSUES COMMANDS TO SV4-6, 8-10, OR 12-14, AS APPROPRIATE, TO VENT EM TO VACUUM RESOURCE OR VACUUM EXHAUST SYSTEM	FOR SV5 FAILURE : SV4 AND SV6 AND ASSOCIATED PATH FOR SV9 FAILURE : SV8 AND SV10 AND ASSOCIATED PATH FOR SV13 FAILURE : SV12 AND SV14 AND ASSOCIATED PATH	SV5, 9, OR 13 OPEN/CLOSE DISCRETE (PRIME) - (PT4, VS1-PT6, VS2-PT8, VS3, PT6, PT7, PT9) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) ACCOMMODATES 2 FAULT TOLERANT FUNCTIONAL FAILURE REQUIREMENT TIME CRITICALITY NEEDS MORE ANALYSIS) APPEARS, THOUGH, THAT S/W LOGIC/CONTROL IS MANDATORY

CONCLUSION: REDUNDANT COMPONENTS AND PATHS IN PLACE SIMULATION OF FAILURE(S) IN SIM LAB/TEST BED IS REQUIRED

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP VACUUM VENT ASSEMBLY
DRAWING SCHEMATIC --
REF DES --

MISSION PHASE
____ PRE-LAUNCH
____ ASCENT
____ DEPLOYMENT
X OPERATIONS
____ CONTINGENCY/RETURN

FF NO 5 a PAGE 1
DATE 12 - 14 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
5 a	5 a	F3, F4, OR F5 CLOGS	PREVENTS EM GAS FOLW TO ACCUMULATOR OR TO VRS/VES POSSIBLY RESULT IN LOSS OF EXPERIMENT	1 SEC (1 S/S PT5, 7 OR 9)	TBD - INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO 5 a PAGE 2

DATE, 12-14-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	SINCE EM OVER PRESSURE RELIEF IS ACCOMMODATED BY BACK UP COMPONENTS AND PATH - PENDING ADDITIONAL ANALYSIS OF EM PRESSURE/VACUUM REQUIREMENTS- T/S F3, 4 OR 5 (MANUAL PROCEDURE)	NONE- (OVER PRESSURE RELIEF IS AVAILABLE)	PT5, 7 AND 9 (PRIME) TBD (EM FURNACE MEASUREMENTS) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO): NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE.
TIME CRITICALITY NEEDS MORE ANALYSIS. NEED FOR S/W DETECTION, ISOLATION, AND RECOVERY IS PENDING.

CONCLUSION: NO REDUNDANT COMPONENTS /PATHS IN DESIGN. REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED ISPENDING.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP VACUUM VENT ASSEMBLY
DRAWING SCHEMATIC -
REF DES -

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 5b PAGE 1

DATE 12 - 14 - 95

FF NO. (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
5 b	5 b	FAILS TO PROVIDE EM PRESSURE RELIEF TO VES (RV1-RV2) EM1 (RV3-RV4) EM2 (RV5-RV6) RIR EM	-FAILS TO RELIEVE EXCESS EM PRESSURE - POSSIBLE DAMAGE TO EM FURNACE/EXPERIMENT	1 SEC (1 S/S - PT4)	TBD- INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FFNO 5 b PAGE 2

DATE 12-14-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	SINCE REDUNDANCY IS PROVIDED - UNLESS ADDITIONAL ANALYSIS OF EM FURNACE DICTATES OTHERWISE T/S (RV1-RV2) (RV3-RV4) OR (RV5-RV6) BY MANUAL PROCEDURE	RV3 - RV4 AND PATH (REDUNDANT) RV1 - RV2 AND PATH (REDUNDANT) RV5 - RV6 AND PATH (REDUNDANT)	PT4/VS1 (PRIME) TBD (EM FURNACE MEASUREMENT) (BACK UP) PT6/VS2 (PRIME) TBD (EM FURNACE MEASUREMENT) (BACK UP) PT8/VS3 (PRIME) TBD (EM FURNACE MEASUREMENT) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO): ACCOMMODATES 2 FAULT TOLERANT FUNCTIONAL FAILURE REQUIREMENT. TIME CRITICALITY NEEDS MORE ANALYSIS - PROBABLY NO S/W LOGIC/CONTROL IS REQUIRED - BUT - MORE EM FURNACE ANALYSIS NEEDED.

CONCLUSION: REDUNDANT COMPONENTS/PATHS ARE IN PLACE.
SIMULATIONS OF FAILURES IN SIM LAB/TEST BED IS PROBABLY REQUIRED

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP VACUUM VENT ASSEMBLY
DRAWING SCHEMATIC -
REF DES -

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 5c PAGE 1
DATE 12 - 14 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
5 c	5 c	SV4, 8, OR 12 FAILS TO OPERATE	LOSS OF EM GAS VENTING CAPABILITY WITH POSSIBLE DAMAGE TO FURNACE	1 SEC (1 S/S) (PT4, VS1) (PT6, VS2) (PT8, VS3)	TBD- INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FFNO 5 c PAGE 2

DATE: 12-14-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	SINCE REDUNDANT CAPABILITY EXISTS - T/S SV4, 8, OR 12 BY MANUAL PROCEDURE	SV4 - SV5 AND PATH (REDUNDANT) SV18- SV9 AND PATH (REDUNDANT) SV12 - SV13 AND PATH (REDUNDANT)	PT4/VS1 (PRIME) TBD (EM MEASUREMENTS) (BACK UP) PT6/VS2 (PRIME) TBD (EM MEASUREMENTS) (BACK UP) PT8/VS3 (PRIME) TBD (EM MEASUREMENTS) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO): ACCOMMODATES 2 FAULT TOLERANT FUNCTIONAL FAILURE REQUIREMENTS TIME CRITICALITY NEEDS MORE ANALYSIS - PROBABLY NO S/W LOGIC/CONTROL IS REQUIRED - BUT - MORE EM FURNACE ANALYSIS NEEDED.

CONCLUSION: REDUNDANT COMPONENTS/PATHS ARE IN PLACE
SIMULATIONS OF FAILURES IN SIM LAB/TEST BED ARE PROBABLY REQUIRED

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP VACUUM VENT ASSEMBLY
DRAWING SCHEMATIC -
REF DES -

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 5d PAGE 1
DATE 12 - 14 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
5 d	5 d	1) SV6, 10, OR 14 FAILS TO OPERATE 2) MV4, 5, OR 6 FAILS TO OPERATE	1) LOSS OF CONTROL TO EXHAUST GAS FROM EM (OR ACC) TO VRS OR VES 2) SAME AS 1) ABOVE POSSIBLY RESULTING IN LOSS OF EXPERIMENT	1 SEC (1 S/S PT5, PT7, OR PT9)	TBD- INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FFNO 5 d PAGE 2

DATE, 12-14-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	SINCE NO REDUNDANT CAPABILITY EXISTS - T/S SV6, 10, OR 14 PER MANUAL PROCEDURE	NONE	PT5 (PRIME) TBD (EM MEASUREMENT) (BACK UP) PT7 (PRIME) TBD (EM MEASUREMENT) (BACK UP) PT9 (PRIME) TBD (EM MEASUREMENT) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE REQUIREMENTS.
TIME CRITICALITY NEEDS MORE ANALYSIS - NEED FOR S/W DETECTION, ISOLATION, AND RECOVERY IS PENDING.

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN
REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING.

FUNCTIONAL FAILURE-DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM SSFF
SUBSYSTEM/ASSY GDS
COMPONENT/EQUIP VACUUM VENT ASSEMBLY
DRAWING SCHEMATIC -
REF DES -

MISSION PHASE
PRE-LAUNCH
ASCENT
DEPLOYMENT
X OPERATIONS
CONTINGENCY/RETURN

FF NO 5e PAGE 1
DATE 12 - 14 - 95

FF NO (1)	FUNCTION DESCRIPTION (2)	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION
5.e	5.e	DCV 2, 4, OR 6 FAILS TO OPERATE	LOSS OF CAPABILITY TO SELECT VENTING CAPABILITY OF EM GAS TO VRS OR VES. RESULTING IN POSSIBLE LOSS OF EXPERIMENT	1 SEC (1 S/S) (PT4/VS1) (PT6/VS2) (PT8/VS3)	TBD- INVOLVES EM FURNACE OPERATION

(1) SEE "FUNCTIONAL FAILURES" TABLE
(2) SEE "BLOCK FUNCTIONS" TABLE

(FF-DAREL)
WORKSHEET
SHEET 2

FFNO 5 c PAGE 2

DATE, 12-14-95

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS
PENDING	SINCE NO REDUNDANCY CAPABILITY EXISTS - T/S DCV2, 4, OR 6 PER MANUAL PROCEDURE	NONE	PT4/VS1 (PRIME) TBD (EM MEASUREMENT) (BACK UP) PT6/VS2 (PRIME) TBD (EM MEASUREMENT) (BACK UP) PT8/VS3 (PRIME) TBD (EM MEASUREMENT) (BACK UP)

SUMMARY-(SIGNIFICANT FAILURE INFO) NOT 2 FAULT TOLERANT FUNCTIONAL FAILURE
TIME CRITICALITY NEEDS MORE ANALYSIS - NEED FOR S/W DETECTION, ISOLATION, AND RECOVERY IS PENDING

CONCLUSION NO REDUNDANT COMPONENTS/PATHS IN DESIGN
REQUIREMENT FOR SIMULATION OF FAILURE IN SIM LAB/TEST BED IS PENDING

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Dec 15, 1995	May 18 - Dec 15, 1995

4. TITLE AND SUBTITLE

SSFF Health Management Analysis Report
Part II (Proof of Concept)

5. FUNDING NUMBERS

NAS8-40365

6. AUTHOR(S)

Lee Wilson, Jim Spruill, Yin Hong

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Alpha Technology
3322 S.Memorial Parkway, Suite 215-H
Huntsville, AL 35801

8. PERFORMING ORGANIZATION REPORT NUMBER

None

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics & Space Administration
Marshall Space Flight Center
MSFC, AL 35812

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Final Report Required by the Contract

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Analysis on SSFF Health Management

14. SUBJECT TERMS

Health Management Follow-Up Study

15. NUMBER OF PAGES

53

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	None	None	