****
* ManTech *
* *
*Document # 40-01-758 *
****
5-11

GN2 BOTTLE RACK-BUILDING 10/15
FAILURE MODES AND EFFECTS ANALYSIS (FMEA)
AND CRITICAL ITEMS LIST (CIL)

Man-Tech Document No.

40-01-758

January 2005

PREPARED BY: 5-6-05
E. Hemminger, Project Engineer — Date
Design & Analysis, ManTech

REVIEWED BY: 5/8/05
W. Rinker, Supervisor — Date
Technical Support Function, ManTech

APPROVED BY: 05/10/05
W. Thomas, Recertification Function, — Date
ManTech

APPROVED BY; 5/17/05
S. Chan, RECERT Program Manager, Code 540, — Date
NASA/GSFC

APPROVED BY; 5/20/05
R. Vernier, Environ. Test Eng., Code 549, — Date
NASA/GSFC

ManTech
International Corporation

Recertification Function
ManTech Aerospace Technology Applications Center
Goddard Space Flight Center
Greenbelt, Maryland 20771

TABLE OF CONTENTS

Page

LIST OF FIGURES ii

LIST OF ATTACHMENTS ii

1.0 SUMMARY OF FINDINGS 1
1.1 System Criticality 1
1.2 Mechanical Critical Items 1
1.3 Electrical Critical Items 1
1.4 Critical Flex Hoses 1
1.5 Critical Orifices 1
1.6 Critical Filters 1
1.7 Criticality Category 1R Items 1
1.8 Critical Control/Monitor Functions 1
1.9 Sneak Circuits Identified 1
1.10 Areas of Concern and Recommendations 1
1.11 Risk Assessment 2

2.0 SYSTEM SUMMARY 2
2.1 Specifications 2
2.2 Documentation List 2

3.0 DEFINITIONS AND GROUND RULES 5
3.1 Definitions 5
3.2 Ground Rules 6

4.0 CRITICALITY ASSESSMENT 8
4.1 Criticality Assessment Worksheets 8

5.0 FAILURE MODES AND EFFECTS ANALYSIS AND CIL 10
5.1 Mechanical FMEA Worksheets 10
5.2 Criticality Category 1R Worksheets 14

6.0 RATIONALE FOR ACCEPTABILITY 16
6.1 Design 16
6.2 Test and Inspection 16
6.3 Failure History 16
6.4 Operational Use 16

7.0 AREAS OF CONCERN AND RECOMMENDATIONS 17

8.0 RISK ASSESSMENT 17

LIST OF FIGURES

Figure	Title	
1.	GN2 BOTTLE RACK- BUILDING 10/15	4

LIST OF ATTACHMENTS

A-	NPR 8715.3 Section 3.6, Hazard Assessment	18

1.0 SUMMARY OF FINDINGS

1.1 System Criticality

The GN2 Bottle Rack-Building 10/15, is assessed as critical. A catastrophic failure of this facility could cause loss of life and/or flight hardware.

1.2 Mechanical Critical Items

There are no critical mechanical items identified by the Failure Modes and Effects Analysis (FMEA).

1.3 Electrical Critical Items

There are no electrical functions associated with this facility.

1.4 Critical Flex Hoses

There are no flex hoses identified to be critical items.

1.5 Critical Orifices

There are no orifices identified to be a Critical Item.

1.6 Critical Filters

There are no filters identified to be a Critical Item.

1.7 Criticality Category 1R Items

There are two Category 1R items identified during the analysis of the critical functions. The 1R items are summarized on the Criticality Category 1R Worksheets, Section 5.2. No single credible cause was identified to result in the loss of the redundant items.

1.8 Critical Control/Monitor Functions

There are no control/monitor functions associated with this system.

1.9 Sneak Circuits Identified

There is no Sneak Circuit Analysis performed for this facility.

1.10 Areas of Concern and Recommendations

Several recommendations are presented to improve the level of protection and minimize or negate the uncertainties identified in the failure modes and effects analysis. In summary, the recommendations address:

- Continuation of Recommended Facility Inspection as specified in General Physics Corporation Report GP-R-570, Table 5-3, Ref. Document Section 2.2. With one exception.
- The one exception is with regard to the bottle clamp bolt re-torque requirement. It is recommended that visual inspection be continued as specified but that bolt re-torque be waived based on justification presented in Section 4.0 Criticality Assessment.
- In addition, continue Recertification of relief valves by way of set-point validation bench testing at 2-year intervals.
- Also, continue removal and replacement of existing carbon steel GN2 Bottle end reducing bushings with Stainless Steel bushings. To minimize facility downtime, it is recommended that this be performed concurrent with relief valve testing at two-year intervals. It is recommended that a minimum 3 bushings be replaced at each interval until all carbon steel bushings have been removed from service.

1.11 Risk Assessment

Risk assessment was performed in accordance with NASA Safety Manual 8715.3. The GN2 Facility is considered safe to operate. The overall risk assessment is determined as follows:

Hazard Severity Level: Class II Critical
Likelihood: Improbable/Remote
Risk: RAC#5 Acceptable

Implementation of the recommendations would <u>add</u> control measures to improve equipment reliability and minimize failure risks.

2.0 SYSTEM SUMMARY

2.1 Specifications

Refer Figure 1, page 4 and Drawing GE-10-19932, Isometric Flow GN2 System Upgrade, Building 10.

2.2 Documentation List

The following documents were used in the performance of this analysis:

1. GP-R-462, Results of Recertification Analysis and Inspection Planning for Priority Group I High Pressure Gas Systems, dated January 31, 1979.
2. GP-R-570, Status Report for Initial Recertification Inspection and Test Implementation for Program RECERT, dated April 30, 1980.

3. NSTS 22206 Revision D, December 10, 1992, Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL).
4. Maintenance History File.
5. NPR 8715.3, latest Revision, NASA Safety Manual.

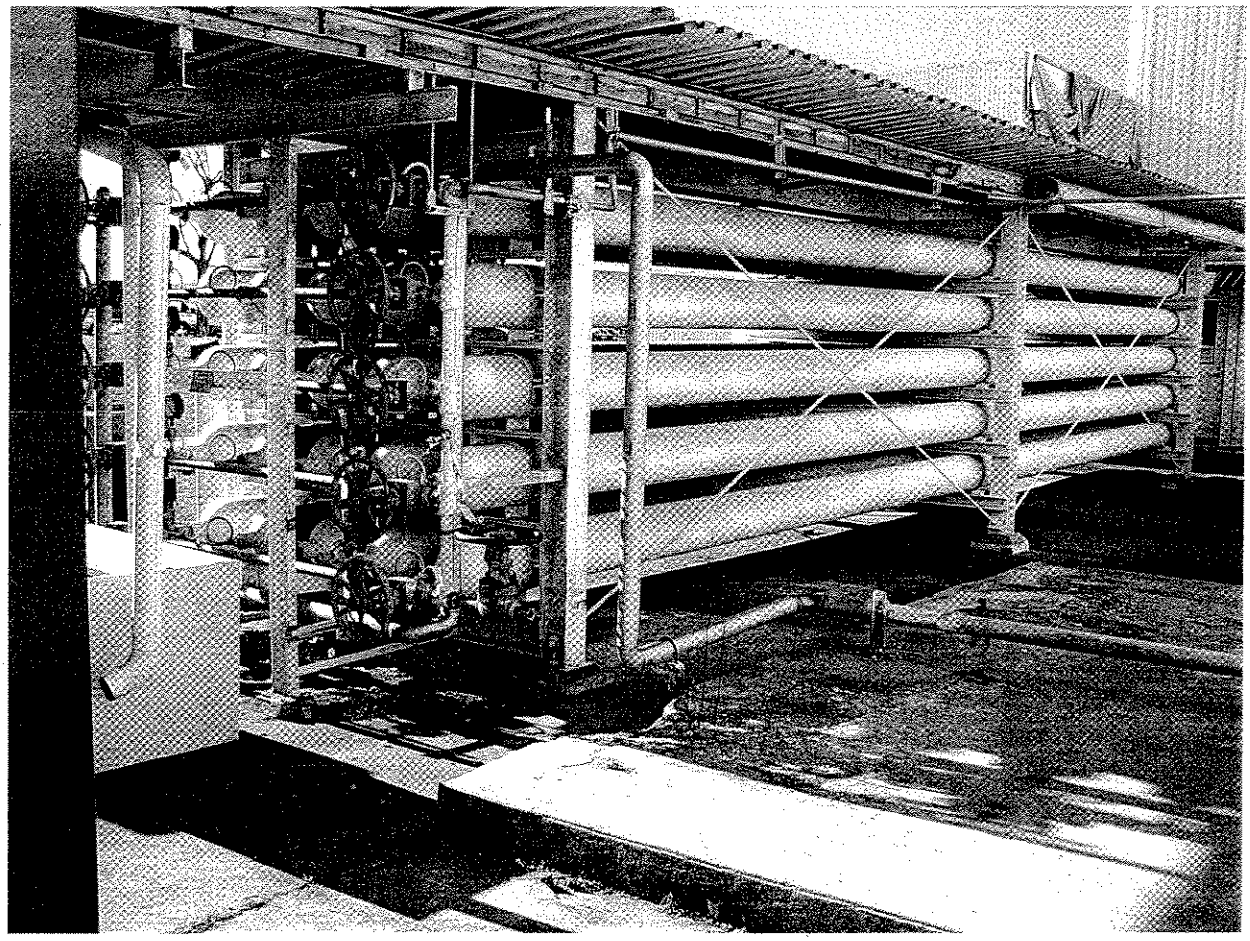

Figure 1

BUILDING 10 GN2 Bottle Rack

3.0 DEFINITIONS AND GROUND RULES

3.1 Definitions

Definitions for the preparation and clarification of the Failure Modes and Effects Analysis are listed below.

Critical Item - A critical item is defined as any one of the following:

1. A Criticality Category 1, 1S or 2 Single Failure Point.

2. A redundant hardware item where the second failure results in loss of life or vehicle and the item is not capable of checkout during normal ground operations (i.e., a single fault tolerant item which fails Redundancy Screen A).

Critical (Reliability Impact) - If loss or improper performance of any one of the system's functions, without regard to redundancy, could result in loss of life or loss of flight hardware or damage to flight hardware, the total system is assessed as Critical. If loss or improper performance of all of the system's functions could not result if any of the aforementioned effects, the system will be considered Non-critical.

Criticality Category

Criticality	Potential Effect or Failure
1	Single failure which could result in loss of life or flight hardware.
1R	Two redundant hardware items, which if both failed, could result in loss of life or vehicle (or loss of a safety or hazard monitoring system).
1S	Single failure in a safety or hazard monitoring system that could cause the system to fail to detect, combat, or operate when needed during the existence of a hazardous condition and could result in loss of life or flight hardware.
2	Single failure which could result in loss (damage) of flight hardware.
3	All others.

Failure Modes and Effects Analysis (FMEA) - A bottoms up systematic, inductive, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the modes of failure. It is usually performed to identify

critical single failure point in hardware. The FMEA is subsidiary to a Hazard Analysis.

Hazard Analysis - A hazard analysis shall, as a minimum, determine potential sources of danger, identify most probable failure modes, and recommend resolutions for those conditions found in the hardware-facility-environment-human relationship that could cause loss of life, personal injury, or loss of lifting device, facility, or load.

Redundancy Screens - Redundancy screens must be addressed for all Criticality Category 1R items. Determination of "Pass," "Fail," or "N/A" (not applicable) must be documented in the summary list of 1R items. The GSE redundancy screens are defined as follows:

(a) Screen A - The redundant item is capable of being checked and verified during normal ground operations.

(b) Screen B - Loss of the redundant item is readily detectable by the operator. (This screen is not applicable to standby redundancy.)

(c) Screen C - Loss of all redundant items cannot result from a single credible cause, such as contamination. It is assumed here that loss of the redundant item(s) is not detectable by scheduled test, inspections, and maintenance nor operator's daily check prior to first use daily.

Time to Effect - The time for the failure effect to occur in this analysis is specified as follows:

ST	Short Term - Months
LT	Long Term - Years

3.2 Ground Rules

This analysis is developed in accordance with NSTS 22206, Revision D, "Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)."

The following ground rules and assumptions are established for this analysis:

a. For this analysis, it is assumed that operation of this facility is performed in accordance with approved operating procedures by trained and certified operators.

b. This analysis assumes worst-case scenario when analyzing Ground Support Equipment (GSE).

c. Passive components are not analyzed in this FMEA, but should be considered in a separate Hazard Analysis, which is not part of this effort.

d. Failures of redundant items which meet the criteria described in 3.1.(a), (b) and (c) above are classified as Criticality Category 1R. Requirements for periodic test, inspection or functional validation of these items are invoked through the appropriate operation and maintenance requirements documentation. Single failure within the system controls which could cause loss of a 1R item is not be identified as 1R but is listed as a cause of the failure of the 1R items which it controls. Such system controls are included in the periodic test, inspection or functional validation requirement invoked on the 1R item.

e. Redundancy screens are addressed for all Criticality Category 1R items. Determination of "Pass," "Fail," or "N/A" (not applicable) are documented in the summary list of 1R items.

f. Failures due to human error in system setup (e.g., manual valves erroneously in the wrong position) are not considered in this FMEA.

g. This analysis assumes that all components, lubricants, fluids and fluid levels are as recommended by the original equipment manufacturer.

h. Fluids

1. Internal leakage is included in the assessment of the "fail open" failure mode.

2. External leakage is considered where leaks are detrimental to system operation or personnel safety.

3. All components located in the system downstream of the final filter are assessed for a possible source of contamination (e.g., transducers, temperature probes, component soft goods).

4. Filters, orifices and flex hoses are analyzed in the FMEA as part of the respective system.

i. The following classification of failure modes, as a minimum, is included in the CIL:

1. All Functional Criticality Category 1 and 2 items.

2. All Functional Criticality 1R items where (1) first failure could result in loss of life and/or flight hardware or (2) next failure of any redundant item could cause loss of operator/lifting device.

3. All Functional Criticality Category 1R items that fail one or more redundancy screens.

j. This FMEA only analyzes the failure modes and effects of the GN2 Bottle Rack components. Other safety issues involving qualification of operating personnel, hazards specific to hi-pressure LN2/GN2 facilities, and provisions for facility protection and emergency recovery during operations, etc., are addressed by specific T/V Facility Operation Procedures.

4.0 CRITICALITY ASSESSMENT

4.1 Criticality Assessment Worksheets

This system input and output functions are assessed on the following Criticality Assessment Summary sheet.

The Criticality Assessment Worksheets are completed to determine whether the GSE is Critical or Non-critical in terms of reliability impact. If loss or improper performance of any one of the system's functions, without regard to redundancy, could result in loss of life or loss of flight hardware or damage to flight hardware, the total system is assessed as Critical. If loss or improper performance of all of the system's functions could not result in any of the aforementioned effects, the system is considered Non-critical.

SYSTEM CRITICALITY ASSESSMENT SUMMARY WORKSHEET				
System GN2 Bottle Rack Facility 259	Drawing See Figure 1, page 4	Location Building 10,15	Prepared by E. Hemminger 1/7/05	
INPUT/OUTPUT	FUNCTION	TIME PERIOD	EFFECT OF LOSS/FAILURE	CRIT. CAT.
Pressure System	Provides gaseous GN2 for operation of Thermal Vacuum Test Chambers.	Storage of pressurized GN2 for T/V Facility operation.	Failure of the Storage Bottle threaded adapters at stagnation pressure of 2400 psi could cause bottles to become projectiles, if restraining clamps fail. (See Section 2.2, item 2.) This could result in loss of flight hardware and or loss of life. Requires multiple failures.	Crit. 1
Restraint System	Provides for bottle structural support and restraint.	Storage of pressurized GN2 for T/V Facility operation.	Failure of the Storage Bottle Restraint during bottle failure at stagnation pressure of 2400 psi could cause bottles to become projectiles, resulting in loss of flight hardware and or loss of life. Requires multiple failures.	Crit. 1

5.0 FAILURE MODES AND EFFECTS ANALYSIS AND CIL

5.1 Mechanical FMEA Worksheets

The various pressure and structural/restraint components of the Facility 259 GN2 Bottle Rack are identified from documents referenced in the Documentation List, Section 2.2 of this Report and are analyzed on the following worksheets.

FAILURE MODE AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Facility 259 GN2 Bottle Rack
DATE: January 7, 2005
SUBSYSTEM: Pressure
PREPARED BY: E. Hemminger
REFERENCE: 1. GE-10-19932 GN2 System Upgrade Drawing, dated 12/27/91
2. GPR 462, Recertification Analysis & Inspection for High Pressure Gas Systems

NO.	PART NAME	FAILURE CAUSE	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON CRITICAL HARDWARE AND/OR PERSONNEL SAFETY	TIME TO EFFECT	CRIT CAT
1	GN2 Storage Bottles 12 in Dia.	Structural defect/corrosion	GN2 leakage with resultant system pressure loss in manifold bank.	Facility ops at reduced capability or shutdown.	LT	3R
2	Relief Valves 1 in Dia.	Structural defect/corrosion	GN2 bypass leakage with resultant system pressure loss in manifold bank.	Facility ops at reduced capability or shutdown.	LT	3R
3	Isolation Valves 1.5 in Dia.	Structural/weld defect/corrosion	GN2 leakage with resultant system pressure loss in manifold bank.	Facility ops at reduced capability or shutdown.	LT	3R
4	Manifold piping 1.5 in sched 80	Structural/weld defect/corrosion	GN2 leakage with resultant system pressure loss in manifold bank.	Facility ops at reduced capability or shutdown.	LT	3R
5	Pressure Gauge 1 in Dia	Broken, out of calibration	GN2 leakage with resultant system pressure loss incorrect reading.	Facility ops at reduced capability or shutdown.	LT	3R

FAILURE MODE AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Facility 259 GN2 Bottle Rack DATE: January 7, 2005
SUBSYSTEM: Pressure PREPARED BY: E. Hemminger
REFERENCE: 1. GE-10-19932 GN2 System Upgrade Drawing, dated 12/27/91
2. GPR 462, Recertification Analysis & Inspection for High Pressure Gas Systems

NO.	PART NAME	FAILURE CAUSE	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON CRITICAL HARDWARE AND/OR PERSONNEL SAFETY	TIME TO EFFECT	CRIT CAT
6	Inlet/outlet Bottle end reducing bushings 1.5 in Dia	Structural Defect, corrosion	GN2 thrust loading possible projectile impact loading.	Could result in severe injury or loss of life, Loss of Facility ops and possible Damage to flight Hardware.	LT	1R

FAILURE MODE AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM Facility 259 GN2 Bottle Rack — DATE: January 7, 2005
SUBSYSTEM: Restraint - Structural — PREPARED BY: E. Hemminger
REFERENCE: GPR 462, Recertification Analysis & Inspection for High Pressure Gas Systems

NO.	PART NAME	FAILURE CAUSE	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON CRITICAL HARDWARE AND/OR PERSONNEL SAFETY	TIME TO EFFECT	CRIT CAT
1	Bottle Clamp Assembly	Loss of Preload on 7/8 dia bolts	Loss of bottle restraint in case of projectile, impact loading. Requires multiple failure.	Could result in catastrophic damage to Building/facility and personal injury	LT	1R
2	6x6 WF Vertical Support Columns	Corrosion, structural degredation	Compromised Stability of Bottle Rack	Could result in structural failure and loss of facility ops.	LT	3R
3	1 in Dia Anchor Bolts	Corrosion, structural degredation	Compromised Stability of Bottle Rack	Could result in structural failure and loss of facility ops.	LT	3R
4	1 in Dia Diagonal Bracing	Corrosion, structural degredation	Compromised Stability of Bottle Rack	Could result in structural failure and loss of facility ops.	LT	3R

5.2 Criticality Category 1R Worksheets

There are two Category 1R items identified during the analysis of the critical output functions. The 1R items are summarized on the following Criticality Category 1R Worksheets.

It is recommended that re-torque of bottle clamps at five year intervals, as recommended by General Physics Inspection & Recertification Requirements, be waived.

Justification for this recommendation is as follows:

- A significant number of bottle clamps have yielded in bending due to the initial pre-load application. It is therefore concluded that bolt re-torque will not insure the application of the General Physics specified restraint force, since clamp yield strength in bending, not bolt torque should be used to calculate restraint.
- Due to paint and rust on threads, loss of preload is not likely. Also this condition would make re-torque operation impossible or at best extremely difficult and cost prohibitive.
- Any preload lost would be compensated for by increased clamp friction coefficient due to rust and paint.

CRITICALITY CATEGORY 1R WORKSHEETS

SYSTEM: Facility 259 GN2 Bottle Rack
SUBSYSTEM'S: PRESSURE & RESTRAINT
REFERENCE: NSTS 22206, Revision D

DATE: January 7, 2005
PREPARED BY: E. Hemminger

NO.	PART NAME	FAILURE CAUSE(S)	FAILURE EFFECT	REDUNDANCY SCREENS		TEST AND INSPECTION REQUIREMENT(S)
				PASS	FAIL	
1	Inlet/outlet Bottle end reducing bushings 1.5 in Dia	Corrosion and or material defect	GN2 leakage/pressure loss or if shear failure could result in projectile/impact loading of bottle.	A B C		• Daily Operator Inspection when in use. • Inspection per Table 5-3, GPR-R-570.
2	Bottle Clamp Assemblies	Loss of clamp/bolt pre-load	Loss of bottle restraint in case of projectile/impact loading.	A B C		• Daily Operator Inspection when in use. • Inspection (1) per Table 5-3, GPR-R-570.

Notes:

(1) Bolt re-torque is not possible due to paint and rust on threads of carbon steel fasteners. It is recommended that bolt re-torque be waived based on the following:

- Due to rust and paint on threaded surface, relaxation of preload is judged highly unlikely.
- Any loss in pre-load would be compensated for by increased friction between clamps and bottle OD due to paint and rust.
- The restraint calculations performed by General Physics and used as basis for re-torque requirement is not complete and therefore suspect.
- The maximum pre-load force is limited by yield strength of clamp flanges in bending and not bolt torque.

6.0 RATIONALE FOR ACCEPTABILITY

No mechanical critical items were retained by the FMEA. The basis for not retaining the critical items is discussed below.

Criticality 1R items <u>are acceptable</u> in that each item is capable of checkout during normal operations. Documentation of the following data elements: Design, Test and Inspection, Failure History and Operational Use are provided to categorize the analysis for risk assessment.

6.1 Design

The GN2 High Pressure Bottle Rack was designed in accordance with applicable Codes such as the ASME Pressure Vessel Code and the AISC Steel Construction Code.

6.2 Test and Inspection

- Daily operator inspection when in use.
- Periodic Inspection and Recertification in accordance with GP-R-570 Table 5-3, with exception of re-torque of bottle clamps as previously discussed.

6.3 Failure History

No Failures have been experienced with regard to this facility.

6.4 Operational Use

Failures due to human error are not considered in the performance of this FMEA. The operation of this facility is subject to certain hazards that cannot be completely eliminated by mechanical means, but the risks can be minimized by the exercise of intelligence, care, and common sense.

It is therefore essential to have competent and careful operators, physically and mentally fit, thoroughly trained in the safe operation and maintenance of the equipment.

Serious hazards are:

- Impact damage to the manifold and or 1.5 inch diameter bottle end reducing bushings while the Facility is pressurized.
- Projectile loading of the damaged bottle, which could become missile if the bottle clamps restraint capability is exceeded.

7.0 AREAS OF CONCERN AND RECOMMENDATIONS

The following recommendations are provided to further improve operational safety and reliability of this high pressure GN2 Facility.

7.1 It is recommended that:

7.1.1 Qualified operators, trained in high pressure GN2 systems, be used for inspection and maintenance of this Facility.

7.1.2 Criticality Category 1R items, identified in this analysis, be included in the Periodic inspection. In particular, reducing bushings and bottle clamps/bolts should be inspected for structural integrity at maximum 2-year intervals.

7.1.3 Carbon Steel reducing bushings, should be replaced with Stainless Steel bushings. This can be accomplished by replacement of 2-3 bushings at 2-year intervals to coincide with facility blow-down for relief valve testing.

7.2 No critical items were retained as a result of this analysis. Two redundant hardware items were identified and are judged capable of checkout during normal operations and maintenance. The time for failure to occur for all components analyzed herein was determined to be "Long Term," i.e., years. Implementation of the aforementioned scheduled test and inspections are recommended to mitigate these respective failure modes. As previously noted, certain hazards such as accidental impact loading of cannot be totally eliminated by mechanical means. However, accidental impact loading is highly unlikely due to the protected location of this facility and the numerous crash barriers imposed by adjacent buildings and facilities/equipment.

8.0 RISK ASSESSMENT

Risk assessment was performed in accordance with NPR 8715.3, Figure 3.2, Risk Assessment Matrix.

Definitions of the "Hazard Severity Levels" and "Likelihood of Occurrence" are defined in the above reference document.

Hazard Severity Level: Class II Critical
Likelihood: Improbable/Remote
Risk: RAC#5 Acceptable (Uncertainties Controlled/Managed)

ATTACHMENT- A

NPR 8715.3 Section 3.6 "Hazard Assessment"

The hazard assessment process is a principal factor in the understanding and management of technical risk. Hazards are identified and resultant risks are assessed by considering probability of occurrence and severity of consequence. Risk may be assessed qualitatively or quantitatively. System safety is an integral part of the overall program risk management decision process. A sample format to document the risk process is provided in Appendix E.

3.6.1 Risk Assessment Code (RAC). The RAC is a numerical expression of comparative risk determined by an evaluation of both the potential severity of a condition and the probability of its occurrence. RAC`s are assigned a number from 1 to 7 in a risk matrix (see figure 3.2.). The RAC number will serve as a means to prioritize corrective actions, e.g., RAC 1 is unacceptable and mitigation actions must be taken immediately or operations terminated, RAC 2`s must be addressed before RAC 3`s, etc. (Requirement 25246). Differences between higher number RAC`s (beyond 4) probably cannot be discerned due to low risk levels. The cognizant safety and program officials may approve variations to the matrix.

3.6.1.1 Severity is an assessment of the worst potential consequence, defined by degree of injury or property damage, which could occur. The severity classifications are defined as follows:

Class I - Catastrophic - A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission.

Class II - Critical - A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware.

Class III - Moderate - A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware.

Class IV - Negligible - A condition that could cause the need for minor first aid treatment though would not adversely affect personal safety or health. A condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear.

3.6.1.2 Probability is the likelihood that an identified hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population. The following is an example of Probability Estimation:

A - Likely to occur immediately. ($X > 10^{-1}$)

B - Probably will occur in time. ($10^{-1} \geq X > 10^{-2}$)

C - May occur in time. ($10^{-2} \geq X > 10^{-3}$)

D - Unlikely to occur. ($10^{-3} \geq X > 10^{-6}$)

E - Improbable to occur. ($10^{-6} \geq X$)

(derived from Mil Std 882-System Safety Program Requirements)

	Probability Estimate				
Severity Class	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

Figure 3.2 Risk Assessment Code Matrix