****
* **ManTech** *
* *
*Document # 40-01-756 *
****

HYDRASET MODEL "O" AUXILIARY HOIST CONTROL FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND CRITICAL ITEMS LIST (CIL)

NSI Document No.

40-01-756

December 2004

PREPARED BY: 12/9/04
E. Hemminger, Project Engineer, Code 540.5 Date
Structural Design & Analysis

APPROVED BY: 12/10/04
W. Thomas, Manager Recertification Support, Date

APPROVED BY; 12/13/04
S. Chan, RECERT Program Manager, Code 540, Date
NASA/GSFC

RECERT Support
NSI Technology Services Corporation
A Subsidiary of ManTech International Corporation
Goddard Space Flight Center
Greenbelt, Maryland 20771

TABLE OF CONTENTS

Page

LIST OF FIGURES AND ATTACHMENTS ii

1.0 SUMMARY OF FINDINGS 1
- 1.1 System Criticality 1
- 1.2 Mechanical Critical Items 1
- 1.3 Electrical Critical Items 2
- 1.4 Critical Flex Hoses 2
- 1.5 Critical Orifices 2
- 1.6 Critical Filters 2
- 1.7 Criticality Category 1R Items 2
- 1.8 Critical Control/Monitor Functions 2
- 1.9 Sneak Circuits Identified 2
- 1.10 Areas of Concern and Recommendations 2
- 1.11 Risk Assessment 3

2.0 SYSTEM SUMMARY 3
- 2.1 Specifications 3
- 2.2 Documentation List 3

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 Summary Worksheet 8

5.0 FAILURE MODES AND EFFECTS ANALYSIS AND CIL 10
- 5.1 Mechanical FMEA Worksheets 10
- 5.2 Criticality Category 1R Worksheet 12

6.0 RATIONALE FOR ACCEPTABILITY 13
- 6.1 Design 13
- 6.2 Test and Inspection 13
- 6.3 Failure History 13
- 6.4 Operational Use 13

7.0 AREAS OF CONCERN AND RECOMMENDATIONS 13

8.0 RISK ASSESSMENT 14

LIST OF FIGURES

Figure	Title	Page
1	HYDRA-SET MODEL "O" Auxiliary Hoist Control	4

ATTACHMENTS

1. NPR 8715.3 Section 3.6, "Hazard Assessment" 15

1.0 SUMMARY OF FINDINGS

1.1 System Criticality

The Hydra-set Model "O" Auxiliary Hoist Control is similar in design to Models A, B, C and D with exception of the lower head. The lower head for this unit does not include piston rod bushing and retention snap ring assembly which is common for all Models A, B, C and D. The specific Model "O" units covered by this FMEA are as follows:

SERIAL #	MODEL	CAPACITY
AO-159	O	1,000 lbs.
AO-169	O	1,000 lbs.

The above units are assessed as critical. Failure of these units could result in personnel injury and or damage/loss of flight hardware. The Type "O" unit design is summarized below:

- This unit <u>does not</u> have a single retaining ring, which could fail under system pressure if not properly seated. The piston rod seal in the lower head of the unit would have to fail under pressure or impact loading for uncontrolled lowering of the payload to occur.
- Four head bolts are used to attach/connect upper and lower cylinder heads to the main body of the unit. Preload on these head bolts is critical since they maintain the upper and lower Hydra-set pressure boundary. If preload were lost on any two of four head bolts, hydraulic fluid leakage and uncontrolled lowering/dropping of the payload could result. The maximum distance of payload lowering/dropping would again be limited to piston travel unless tensile failure or thread tear-out of head bolts were to occur.

1.2 Mechanical Critical Items.

1.2.1 The Lower Head

The lower head in this unit is identified "critical" by the Failure Modes and Effects Analysis (FMEA). The HYDRA-SETS are hydraulically operated and failure of the lower head would result in loss of fluid pressure and Hydra-set lift capability. The payload would drop a maximum distance equivalent to the range of piston travel but no further. Restraint provided by the four head bolts would prevent further piston motion. Controlled payload lowering would be maintained from that point, using the crane, unless Hydra-set structural failure was experienced or the payload was situated at height less than piston travel.

1.2.2 Head Bolts

The four head bolts are also identified "critical" by the FMEA. Loss of preload on these bolts could result in hydraulic pressure loss and uncontrolled lowering of the payload.

1.3 Electrical Critical Items

There are no electrical functions associated with this lifting device.

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 Items.

1.6 Critical Filters

There are no filters identified to be a Critical Items.

1.7 Criticality Category 1R Items

The head bolts are identified as category 1R and are evaluated in 1R Worksheet, 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 are no Sneak Circuits to be analyzed.

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 are as follows:

- Inclusion of Category 1R Items in the Periodic Inspection Procedure.
- Hydra-set Operator Certification on annual basis.

1.11 Risk Assessment

Risk assessment was performed in accordance with NASA Safety Manual NPR 8715.3, Section 3.6 "Hazard Assessment". The Hydra-set Model "O" is considered safe to operate. The overall risk assessment is as follows:

- Hazard Severity Class: II-Critical
- Probability Estimation: E-Improbable
- Risk Assessment: 5-Acceptable

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

2.0 SYSTEM SUMMARY

2.1 Specifications

Refer to the respective "Operation and Maintenance Manuals" Section 2.2 below.

2.2 Documentation List

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

1. NSTS 22206 Revision D, December 10, 1992, "Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)."

2. NASA-STD-8719.9, "Standard for Lifting Devices and Equipment", May 2002 or latest revision.

3. GPR 8719.1, "Certification and Re-certification of Lifting Devices and Equipment."

4. Maintenance History File.

5. NASA Safety Manual NPR 8715.3, Section 3.6 "Hazard Assessment".

6. DEL PUB 85-6 HYDRA-SET MODEL "O" Auxiliary Hoist Control, "Operation and Maintenance Manual.

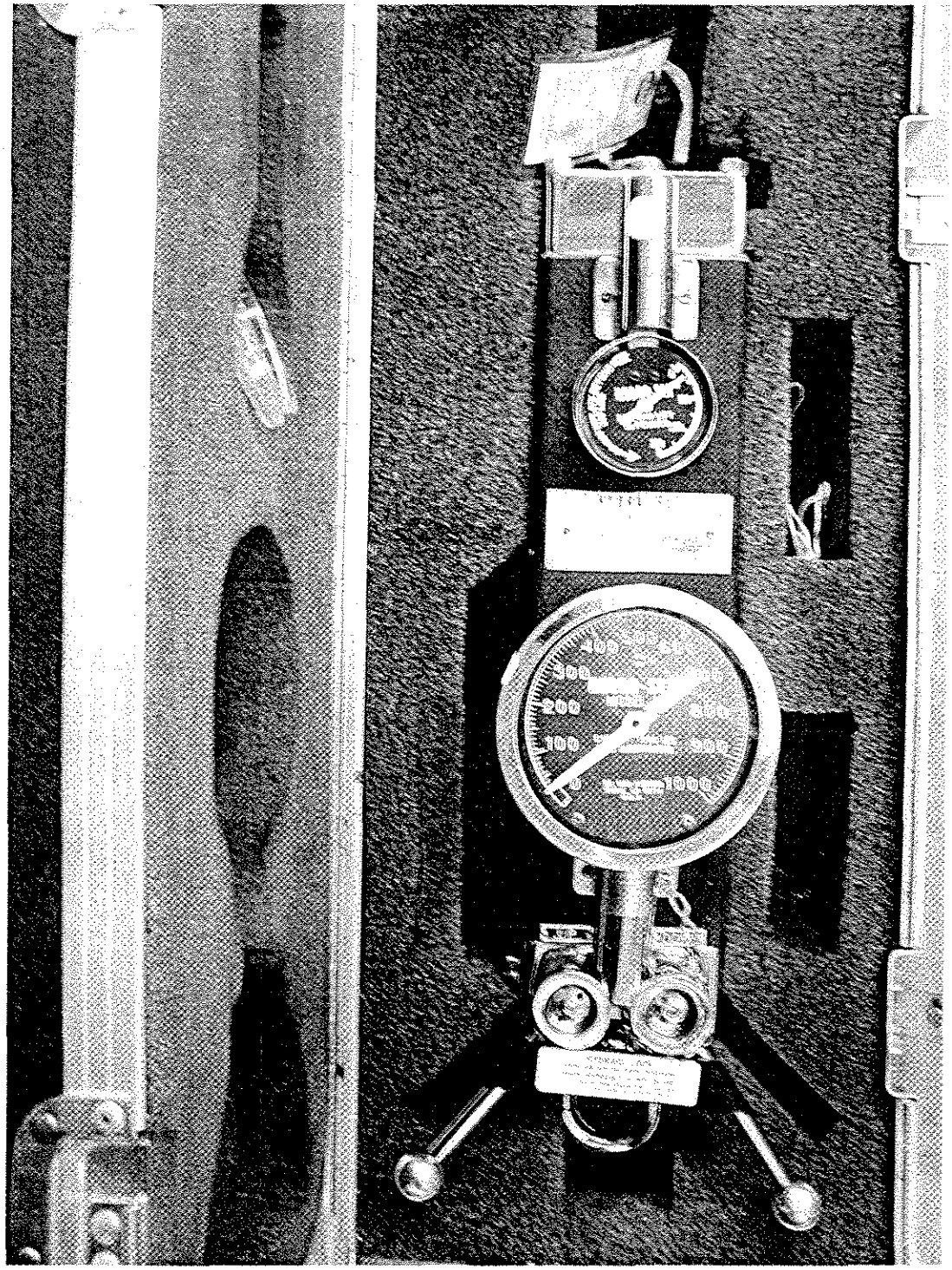

Figure-1 HYDRA-SET Model "O" Auxiliary Hoist Control

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 points 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. Critical lift crane operators are certified annually to operate cranes and Hydra-sets.

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 Hazard Analysis, 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, and hydraulic 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 HYDRA-SET system and components. Other safety issues involving operating personnel qualifications, inherent hazards of a specific critical lift, and provisions for facility protection and emergency recovery during lift operations, etc., to be addressed in the specific Critical Lift Procedure. The Procedure is usually initiated and funded by the Project, if warranted, and developed by integration support personnel.

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 performed 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 HYDRA-SET Model "O"	Drawing See Figure 1, page 4	Location Building 7,10,15 and 29	Prepared by E. Hemminger 12/8/04	
INPUT/OUTPUT	FUNCTION	TIME PERIOD	EFFECT OF LOSS/FAILURE	CRIT. CAT.
Hydraulic Lift System	Provides ability to raise/lower loads up to but not exceeding HYDRA-SET capacity.	Pick up, transport, and deposit of the load.	Failure of the overall lift system could cause the load to drop a maximum distance equal to piston stroke. Could cause personnel injury and or damage/loss of flight payload.	Crit.

5.0 FAILURE MODES AND EFFECTS ANALYSIS AND CIL

5.1 Mechanical FMEA Worksheets

The mechanical components of the HYDRA-SET Model "O" are identified from documents referenced in the Documentation List and are analyzed on the following worksheets.

FAILURE MODE AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: HYDRA-SET Model "O" Auxiliary Hoist Control
SUBSYSTEM: Lift
REFERENCE: HYDRA-SET Model "O" Auxiliary Hoist Control Operation & Maintenance Manual DEL PUB 85-6, Aug. 1988

DATE: December 8, 2004
PREPARED BY: E. Hemminger

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	Hoist inner & outer Cylinders	Surface scratches on fluid surfaces causing by-pass leakage.	Piston rod unloading due to by-pass leakage.	Loss of lift control due to unintentional piston motion.	LT	2
2	Head Upper & Lower Housing Flanges	Distortion, excessive deflection due to pressure and or pre-load application	Piston rod unloading due to by-pass leakage.	Loss of lift control due to unintentional piston motion.	LT	2
3	Cylinder Seal Rings multiple	Surface debris	Hydraulic oil leakage and resultant piston rod unloading.	Loss of lift control due to unintentional piston motion.	LT	2R
4	Plunger Rod Assembly	Excessive wear and scratches on rod surface resulting in seal leakage.	Intermittent piston hang-up and unloading due to leakage.	Loss of lift control due to unintentional piston motion.	LT	2
5	Piston head Tie Bolts multiple	Loss of pre-load on minimum two of four bolts	Hydraulic oil leakage and unloading.	Uncontrolled movement/loss of load. Requires multiple failures.	LT	1R
6	Rod Wiper Assembly	Wear and abrasive damage	Intermittent loss of fluid and resultant unloading.	Uncontrolled movement/dropping the load.	LT	3
7	Pump & Down Valve Ass'y	Wear and abrasive damage	Unable to lift or lower load.	Unable to lift or lower load.	LT	3
8	Lower Eye Roll Pin	Twisted, over-compressed	If roll pin backs out, Lifting Eye could become unthreaded resulting in, loss of load	Requires multiple failures.	LT	2R

FAILURE MODE AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: HYDRA-SET Model "O" Auxiliary Hoist Control
SUBSYSTEM: Lift
REFERENCE: HYDRA-SET Model "O" Auxiliary Hoist Control Operation & Maintenance Manual DEL PUB 85-6, Aug. 1988

DATE: December 8, 2004
PREPARED BY: E. Hemminger

NO.	PART NAME	FAILURE CAUSE	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON CRITICAL HARDWARE AND/OR PERSONNEL SAFETY	TIME TO EFFECT	CRIT CAT
9	Return Force Gauge	Physical damage, hydraulic leakage	Loss of pumping force indication.	Unintentional movement of payload.	LT	2
10	Load Gauge	Physical damage, load sensing failure	Loss of Load sensing.	Could Exceed allowable load.	LT	2

CRITICALITY CATEGORY 1R WORKSHEETS

SYSTEM: HYDRA-SET Model O Auxiliary Hoist Control
SUBSYSTEM: Lift
REFERENCE: NSTS 22206, Revision D

DATE: December 8, 2004
PREPARED BY: E. Hemminger

NO.	PART NAME	FAILURE CAUSE(S)	FAILURE EFFECT	REDUNDANCY SCREENS		TEST AND INSPECTION REQUIREMENT(S)
				PASS	FAIL	
1	Piston Head Tie Bolts	Loss of Preload.	Head bolt joint separation resulting in hydraulic fluid leakage and uncontrolled piston movement/could result in dropping the load.	A B C		• Operator inspection prior to first use daily. • Frequent inspection monthly. • Periodic inspection annually.

6.0 RATIONALE FOR ACCEPTABILITY

The piston head tie bolts were the only mechanical critical items identified by the FMEA. These Criticality 1R items are acceptable in that they are capable of being checked during normal ground 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

HYDRASET design has been verified to be in accordance with applicable ASME/ANSI/ASTM Codes. This insures sufficient design margins are used for all pressure and load bearing parts and requires that proof testing be performed to verify load capacity and workmanship. This design process minimizes the probability of occurrence of the critical failure modes and their causes.

6.2 Test and Inspection

Operator inspection prior to use in addition to Frequent and Periodic Inspection and maintenance per "Test & Inspection, Cleaning and Overhaul Procedure for Manual HYDRA-SET Positioning Devices", Man-Tech Document #40-06-186-3.

6.3 Failure History

No failures have been experienced for this model HYDRA-SET.

6.4 Operational Use

6.4.1 Failures due to human error are not considered in the performance of a failure modes and effects analysis. This factor is minimized by way of certification training as recommended in section 1.10.

7.0 AREAS OF CONCERN AND RECOMMENDATIONS

The following recommendations are provided to further improve operational safety and reliability of this equipment for flight project support.

7.1 It is recommended that:

7.1.1 Critical HYDRA-SET inspections be performed by certified personnel only.

7.1.2 All Critical and Criticality Category 1R items identified in this analysis be included in the

Frequent (monthly) and Periodic (annual) inspections.

7.1.3 Frequent and Periodic inspections be performed according to approved RECERT inspection procedures only.

7.2 All critical item identified as a result of this analysis will be checked during frequent monthly inspections and prior to normal use.

All redundant hardware items identified are capable of checkout during normal operations. The time for failure to occur for these components was determined to be "Short Term," i.e., months. Implementation of the aforementioned scheduled test and inspections are recommended to mitigate these failure modes.

Operators trained in the safe operation of the equipment can minimize the risk of human error. The risk of human error is further reduced by the center requirement which mandates crane operators attend annual refresher training on use of cranes and Hydra-sets.

8.0 RISK ASSESSMENT

Risk assessment was performed in accordance with NASA Safety Manual NPR 8715.3, Section 3.6 "Hazard Assesment". The HYDRA-SET Model O is considered safe to operate. The overall risk assessment is as follows:

- Hazard Severity Class: II-Critical
- Probability Estimation: E-Improbable
- Risk Assessment: 5-Acceptable

Rationale for acceptability is discussed in Section 6.

ATTACHMENT-1

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