MSC-00189

SPACE STATION SAFETY STUDY

SUBSYSTEM ANALYSIS

D2-113070-11

JANUARY 1970

N70-20812
(ACCESSION NUMBER) (THRU)
88 1
(PAGES) (CODE)
CR-108287 31
(NASA CR OR TMX OR AD NUMBER) (CATEGORY)
FACILITY FORM 602

NATIONAL AERONAUTICS & SPACE ADMINISTRATION
MANNED SPACECRAFT CENTER
HOUSTON, TEXAS

THE BOEING COMPANY
AEROSPACE SYSTEMS DIVISION, SEATTLE, WASHINGTON

NASA CR 108287

SPACE STATION SAFETY STUDY MSC-00189

SUBSYSTEM ANALYSIS

D2-113070-11

Prepared for
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
MANNED SPACECRAFT CENTER
Houston, Texas

CONTRACT NAS9-9046

January 1970

TECHNICAL DIRECTION

NASA

Frank S. Coe
STUDY TECHNICAL MONITOR

Rene A. Berglund
ADVANCED PROJECTS OFFICE

Jack W. Wild
NASA HEADQUARTERS

Boeing

William N. Gilbert
SYSTEM OPERATIONS AND DESIGN

Edward P. Goodrich
SYSTEMS ANALYSIS

Earl L. McCabe
STUDY MANAGER

Boeing Approval Earl L. McCabe
E. L. McCabe

AEROSPACE SYSTEMS DIVISION THE BOEING COMPANY SEATTLE, WASHINGTON

PREFACE

This document constitutes one volume of the final report prepared under Contract NAS9-9046, Space Station Safety Study, which was conducted by the Aerospace Systems Division, Aerospace Group, The Boeing Company, under the direction of the Advanced Projects Office, Advanced Missions Program Office, Manned Spacecraft Center, NASA. The objective of the study was to develop a management tool for evaluating conceptual designs of future manned space systems from a safety viewpoint. This objective was achieved through the application of methodical techniques, which are described where necessary in appropriate volumes of this final report, for analyzing space station safety problems. This work resulted in the development of Crew Safety Guidelines which can be used in evaluating future space station concepts.

In Phase I of the study, the work was directed toward a broad class of space stations, using several specific configurations as examples, and considering both crew safety and mission accomplishment as safety goals. In May 1969, the study was redirected by NASA into Phase II to provide more direct support to the NASA Phase B Future Space Station Study, considering only crew safety as the safety goal. To the extent possible, the work done in Phase I was revised and adapted to Phase II and all documents of this final report, except as otherwise noted, include the results from both phases. In both phases the study scope included only on-orbit operations and not launch, boost, de-orbit, and recovery operations, or any operations of the logistics support system, except for close-in rendezvous and docking operations.

The approach taken in the study was to examine the space station from the viewpoint of safety only, with the intent of identifying as complete a list as possible of those measures which should be taken to maximize crew safety. Also, and especially in Phase II, the study dealt primarily with station concepts, rather than specific designs or hardware items. It was not possible, and no attempt was made, to examine the impact of safety measures on other important aspects of space station development, such as cost, design difficulty, or operational suitability. As station development proceeds, trade studies between safety measures and other factors will be required and management decisions must be made as to the extent to which other desirable features will be permitted to override safety measures.

The documents constituting the final study report are:

- D2-113070-4, Condensed Summary Report
- D2-113070-5, Crew Safety Guidelines, Volumes I and II

- D2-113070-6, Supporting Analyses
    - Analysis of Operations
    - Experiment Program
    - Traffic Patterns Analysis
    - Human Requirements
    - Meteoroid Penetration
- D2-113070-9, Logic Diagram
- D2-113070-10, Fault Tree Analysis
- D2-113070-11, Subsystems Analysis

Other documents produced during the study but not part of the final report are:

- D2-113070-1, Detail Study Plan (Phase I only)
- D2-113070-2, Midterm Oral Report
- D2-113070-3, Final Oral Report
- D2-113070-7, Baseline Mission Description (Phase I only)
- D2-113070-8, Baseline System Description (Phase I only)

The references applicable to this document are shown in Section 4.0. However, all the references for those documents which comprise the final study report are compiled in D2-113070-5.

ABSTRACT

An analysis of generic subsystems that must be included in a spacecraft for a long-duration, manned, Earth-orbital mission was performed to identify potential hazards to crew safety, and the possible causes and effects of these hazards. The causes and effects were analyzed to determine appropriate safeguards which would prevent or contain the potential hazards identified. Safety guidelines were written which encompassed all of the recommended safeguards. These guidelines are referenced in Section 3.3 of this document opposite the safeguards to which they pertain, and the guidelines themselves are provided in D2-113070-5 of this report.

KEY WORDS

crew safety

failure analysis

hazards

safeguards

safety analysis

safety guidelines

subsystem analysis

PRECEDING PAGE BLANK NOT FILMED

TABLE OF CONTENTS

Section	Title	Page
	Preface	iii
	Abstract and Key Words List	v
	Table of Contents	vii
	List of Tables	ix
1.0	Introduction	1
2.0	Phase I Subsystems Analysis	3
3.0	Phase II Subsystems Analysis	5
4.0	References	39
Appendix A	Phase I Failure, Safety and Maintenance Analysis Data Sheets	45
Appendix B	Applicable Logic Diagram and Fault Tree Statements	71

PRECEDING PAGE BLANK NOT FILMED

LIST OF TABLES

		Page
3.2-1	Communications and Data Management System Hazard Summary	6
3.2-2	Crew System Hazard Summary	7
3.2-3	Electrical Power System Hazard Summary	8
3.2-4	Environmental Control/Life Support System Hazard Summary	9
3.2-5	Stability and Control System Hazard Summary	10
3.2-6	Structures/Mechanical Systems Hazard Summary	11
3.3-1	Communications and Data Management Safeguards	13
3.3-2	Crew System Safeguards	15
3.3-3	Electrical Power System Safeguards	21
3.3-4	Environmental Control/Life Support System Safeguards	25
3.3-5	Stability and Control System Safeguards	34
3.3-6	Structures/Mechanical Systems Safeguards	37

1.0 INTRODUCTION

1.1

Subsystem analyses performed during the Space Station Safety Study consisted of two separate efforts, Phase I and Phase II. In the Phase I part of the study, the subsystems analysis was conducted as a Failure, Safety and Maintenance Analysis on each subsystem. The subsystems analyzed were based on the Saturn V Single Launch Space Station Study (Reference No. 80). This analysis was about 50 per cent completed when the study redirection resulted in its cessation.

1.2

The Phase II part of the study required a subsystems analysis oriented to the identification of hazards which could threaten crew safety. Safeguards necessary to prevent or contain these hazards were then recommended. Safety guidelines based on the recommended safeguards are included in Document D2-113070-5, Crew Safety Guidelines. This Phase II analysis was not constrained to any particular space station configuration. However, most of the work previously accomplished in Phase I was applicable and was used as a baseline for the Phase II effort.

PRECEDING PAGE BLANK NOT FILMED.

2.0 PHASE I SUBSYSTEMS ANALYSIS

2.1 ANALYSIS

This analysis was based on the space station subsystems used in the Saturn V Single Launch Space Station Study (Reference No. 80) and incorporated in the Baseline System Description document, D2-113070-8. A Failure, Safety and Maintenance Analysis was performed at the component level for each of these subsystems. Each of the components was examined as to its function within the subsystem and its relationship to other elements of the subsystem as well as to other subsystems. Reference No. 80 was the primary source of information for descriptions of the subsystems and their components. In addition, numerous other studies which used comparable subsystems were examined to obtain additional information for the analysis. The other data sources are included in the reference list in Section 4.0. Based on the information available, each component was reviewed for failure modes which could result in a potential hazard to the crew or mission. The potential hazards were analyzed to identify the safety provisions which were already included in the baseline system, or should be considered, to prevent or alleviate the hazard. Each condition was further examined for methods of detecting these critical failures and the maintenance requirements for correcting the failure.

2.2 STATUS AND DOCUMENTATION

The analysis was documented on a form which combined the required failure, safety and maintenance data. This analysis would have involved a number of iterations before completion. At the time of study redirection (the end of Phase I) the first iteration of the subsystem analysis had been done on the following subsystems: Communications and Data Management, Crew System, Electrical Power, Stability and Control, and about 50 per cent of the Environmental Control/Life Support System. The analysis forms for the work completed are included in Appendix A, together with a description of the columns used in the form and the rationale used in completing the form.

PRECEDING PAGE BLANK NOT FILMED.

3.0 PHASE II SUBSYSTEM ANALYSIS

3.1 ANALYSIS

Study redirection changed the scope of the subsystems analysis considerably. The study concept in Phase II was more universal in nature than that of Phase I, which was directed to specific spacecraft configurations. The objective of the redirected study effort was to establish safety guidelines for crew safety only. In keeping with this objective, the potential hazards and safety provisions aspects of the Phase I subsystems analysis were reviewed. The potential hazards, possible causes, and effects identified in that analysis, were summarized as presented in Paragraph 3.2 below. The Phase I analysis was not completed and only one specific space station configuration was examined. Therefore, considering the more universal nature of Phase II of the study, it was necessary to expand the hazard summary to include consideration of other subsystem configurations. To the extent possible, all of the appropriate references of Section 4.0 were reviewed. The subsystem data available were analyzed for potentially hazardous situations which were considered inherent in the equipment or associated with its operation. As the potential hazards were identified, they were analyzed to determine what safeguards should be considered to prevent or alleviate the hazard. The recommended safeguards are presented in Paragraph 3.3. These safeguards formed a basis upon which definitive safety guidelines were written for inclusion in the Crew Safety Guidelines document, D2-113070-5.

3.2 HAZARD SUMMARY

The following tables summarize the potential hazards identified from an analysis of each subsystem as described in Paragraph 3.1. The "Cause" column lists possible events or failures which could produce the potential hazard. The "Effect" column lists the possible effects resulting from an occurrence of the potential hazard. These effects may be either primary or secondary.

TABLE 3.2-1

COMMUNICATIONS AND DATA MANAGEMENT SYSTEM HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. Loss of external voice communications	Transmitter failure Receiver failure Premodulation processor failure Antenna failure	Cannot talk to ground Cannot talk to EVA crew Cannot talk to logistics vehicles Cannot talk to independent modules
2. Loss of internal voice communications	Failure of one or more audio centers Microphone failure Headset failure	Cannot talk to all crew members in space station
3. Loss of data communication with ground	Up-data receiver-decoder failure Premodulation processor failure Telemetry failure	Loss of automatic up-date information Loss of ground command capability Cannot transmit data to ground
4. Loss of time reference	Timing unit failure Up-data receiver-decoder failure	Degraded performance of all time-referenced equipment; e.g., computer functions, a.c. power regulation
5. Loss of computer function	Data adapter failure Computer failure Power supply failure	Degraded performance of spacecraft systems and experiments Loss of data

TABLE 3.2-2

CREW SYSTEM HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. EVA equipment failure	Pressure suit leakage Cooling circuit failure CO_2 removal failure	Crew injury or loss
2. Food contamination	Cooling system failure Water contamination Inadequate storage	Crew illness Food shortage
3. Radiation	Inadequate protection Excessive time in orbit RF radiation	Crew injury or loss
4. Crew injury or illness	Inadequate interior design Inadequate restraint provisions Inadequate crew operating procedures Inadequate crew warning system	Increased workload on remaining crew Possible emergency treatment
5. Inadequate maintenance capability	Lack of replacement parts Lack of maintenance instructions Failure or lack of maintenance equipment	Degraded system operation Limited mission duration Emergency support required

TABLE 3.2-3

ELECTRICAL POWER SYSTEM HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. Fire, smoke, toxic products	Short circuits Electrical overload Arcing Battery overpressure Overheating	Atmosphere contamination Crew injury or illness Equipment damage
2. Loss of electrical power	Power source failure Charging system failure Distribution system failure Power conversion system failure Thermal control failure Solar panel damage	Loss of a.c. power Loss of d.c. power Loss of electrical equipment operation
3. Power source radiation	Thermal control failure Shielding failure Inadequate shielding	Crew illness or injury Electronic equipment malfunction Seal damage Propellant damage

TABLE 3.2-4

ENVIRONMENTAL CONTROL/LIFE SUPPORT SYSTEM HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. Loss of O_2	Regulator failure Tank leakage Valve failure Plumbing failure Thermal control failure	Crew illness Decreased mission duration Danger of fire O_2 shortage
2. Loss of cabin pressure	Cabin leakage Structural damage Regulation failure Seal failure	Crew injury Loss of cabin air supply
3. Excessive CO_2	CO_2 removal failure Excessive CO_2 generation Excessive humidity	Crew illness
4. Fluid leakage	Plumbing failure Component failure Seal failure	Contamination Fire danger Equipment damage
5. Atmosphere contamination	Filter clogged or failed Fluid leakage Fire, smoke Contaminant removal failure Air circulation failure	Crew illness Equipment damage
6. Loss of thermal control	Component failure Radiator failure Control failure Air circulation failure Heater failure	Too hot or cold Freezing fluid lines Equipment damage Unusable O_2 supply
7. Water contamination	Purification failure Valve failure Improper cleaning Tank failure	Crew illness Water shortage
8. Loss of suit loop	Valve failure Component failure Purification failure Regulation failure	Not available in emergency

TABLE 3.2-5

STABILITY AND CONTROL SYSTEM HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. Loss of attitude control	Propellant supply failure Thruster assembly failure Shutoff valve failure CMG failure Electronics failure Manual attitude control failure Excessive docking loads BMAG failure	Spacecraft tumbling Loss of solar panel orientation Crew disabled Loss of experiment data
2. Propellant leakage	Shutoff valve failure Plumbing failure Relief valve failure Tank failure	Loss of propellant Contamination of other equipment Possible fire
3. Propellant tank rupture	Meteoroid penetration Collision with other objects Tank overpressure	Damage to spacecraft or other equipment Injury to personnel Possible fire
4. Exhaust plume	Inherent to spacecraft systems	Damage to equipment or EVA personnel
5. Fire	See 2. and 3. above	Damage to equipment Injury to personnel

TABLE 3.2-6

STRUCTURES, MECHANICAL SYSTEMS HAZARD SUMMARY

Potential Hazard	Cause	Effect
1. No airlock capability	Seal failure Pressurization failure Hatch failure Pumpdown failure	Restricts EVA Restricts crew transfer Loss of atmosphere Crew injury
2. Docking accident	Control system failure Docking equipment failure Lighting failure	Space vehicle structural damage Damage to exterior equipment Damaged docking port Crew injury Cannot accomplish docking Cabin pressure loss
3. Cannot transfer resupply cargo	Docking port damage Transfer equipment failure	Restricted mission duration
4. Structural damage	Micrometeoroid penetration Faulty handling and movement of equipment Long-term micrometeoroid bombardment Space debris Collision	Cabin pressure loss Equipment damage Crew injury or loss

3.3 RECOMMENDED SAFEGUARDS

3.3.1

Recommended safeguards are presented in this section for each of the potential hazards identified in Paragraph 3.2. The safeguards given here are those that could be provided to preclude the potential hazard from occurring, or to prevent an adverse condition from developing into a hazardous situation. It should be borne in mind that a subsystem analysis is based on hardware concepts, and thus is subject to many of the limitations and constraints involved in definition of that hardware. Also, the fact that hardware configurations, however preliminary, are being analyzed implies a much lower level of detail than was possible to achieve in most areas of the Logic Diagram or the Fault Tree during the current study. On this account it might appear that the cross-references to those analyses, as listed here, occasionally are rather tenuous, but it is believed that hardline relationships could be derived quite easily with a modicum of additional logical development. The value of the cross-references lies, of course, in the fact that the other analyses, which were performed more or less independently from each other, provide supporting considerations for the guidelines derived.

3.3.2

Entry codes on the following safeguard tabulations are as follows:

a. An entry in the "Analysis Reference" column identifies the number of a block in the Logic Diagram (D2-113070-9) or Fault Tree (D2-113070-10) which is associated with this safeguard and its derivative guideline. For example, "FT 1.2-B" refers to Fault Tree No. 1, Chart 2, event "B," and "LD-15K" refers to Logic Diagram Chart 15, proposition "K." For convenience, verbatim transcripts of the statements referenced here are given in Appendix "B" of this document, but it is recommended that the appropriate documents be consulted to determine the proper contexts and relationships of the statements quoted.

b. The "Doc. Ref." column contains reference numbers of the documents listed in Section 4.0 which discuss or make recommendations similar to those given in the safeguards.

c. The "Applic. Guideline" column identifies the number of the safety guideline contained in D2-113070-5 that incorporates this safeguard. Some of the more general safeguards have been mentioned in a number of references; in these cases, only one or two of the more prominent or detailed treatments are listed in this column.

TABLE 3.3-1

SYSTEM: 1. Communications and Data Management		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	**Recommended Safeguards**			
1.1 Loss of external voice communications	1.1.1 Provide redundancy for essential space-to-Earth communications equipment, including antennas.	LD-10F	80	12.32
	1.1.2 Provide redundancy for communications between a space station and logistics vehicles, EVA personnel, and independent modules.	LD-10F	80	12.32
	1.1.3 Provide commonality of voice communications equipment in logistics or Earth-return vehicles with that of the space station.	LD-9D		12.12
	1.1.4 Provide multiple power paths to voice communications equipment.	LD-10F		4.9
1.2 Loss of internal voice communications	1.2.1 Provide at least one intercom station in each space station compartment, including airlocks.	LD-9C		12.44
	1.2.2 Provide visual warning at central console whenever an intercom station failure occurs.	LD-18D		12.41
	1.2.3 Provide an independent emergency communications system for directing and controlling operational activities in emergency situations.	LD-10F		12.24
1.3 Loss of data communication with ground	1.3.1 Provide redundancy for Earth-to-space command capability.	LD-4D		12.32
	1.3.2 Provide redundancy for critical space-to-Earth data communication equipment, including antennas.	LD-10F		12.32

SYSTEM: 1. Communications and Data Management (Page 1 of 2)

TABLE 3.3-1 (cont.)

SYSTEM: 1. Communications and Data Management (cont.)			Analysis Reference	Doc. Ref.	Applic. Guidelines
Potential Hazard		Recommended Safeguards			
1.3	Loss of data communication with ground (cont.)	1.3.3 Provide commonality of data communications equipment in logistics or Earth-return vehicles with that of the space station.	LD-9D		12.12
		1.3.4 Provide multiple power paths to data communications equipment.	LD-10F		4.9
1.4	Loss of time reference	1.4.1 Provide redundancy for timing equipment and for up-date capability for timing equipment.	LD-10F	50 98	12.60
1.5	Loss of computer function	1.5.1 Provide redundancy for all computer and data adapter modules.	LD-10F	80	12.15
		1.5.2 Provide multiple power paths to computer equipment.	LD-10F		4.9
		1.5.3 Provide alternate modes of operation as backup for critical computer functions.	LD-10F		12.15
		1.5.4 Include provisions to avert malfunctioning of critical computer functions if a power failure occurs.	LD-10D		4.9

SYSTEM: 1. Communications and Data Management (Page 2 of 2)

TABLE 8.1-1

SYSTEM: 2. Crew System		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	**Recommended Safeguards**			
2.1 EVA equipment failure	2.1.1 Provide monitoring capability for pressure suit O_2 usage to detect suit leakage.	FT 1.2-B LD-15K	78	8.21
	2.1.2 Provide a repair capability for pressure suit seals or minor damage to suit pressure fabric.	FT 1.1-G LD-33E	1 43	5.11
	2.1.3 Monitor CO_2 level of suit and provide visual, audible warning to suited person and also to space station central console if maximum CO_2 level is exceeded.	LD-18D -45E	78	8.20
	2.1.4 Monitor temperature and humidity levels inside suit and provide visual/audible warning to suited person and to space station central console if levels exceed specified limits.	LD-18D -44B, D		8.23
	2.1.5 Use "buddy" system for EVA, i.e., always have two men in pressure suits so that one can immediately help the other in case of emergency.	FT 1.1-G LD-28C, G		12.48
	2.1.6 Design pressure suits to operate at pressures and gas compositions which will minimize the denitrogenation requirements in making the transition from the cabin atmosphere to the pressure suit atmosphere.	LD-44C, E	50 68 77	8.19
	2.1.7 Provide emergency backup to PLSS to enable EVA crew members to return to space station airlock in case of PLSS failure.	FT 1.1-F LD-8C -18D -33I	27	3.16
	2.1.8 Provide redundant pressure suits and PLSS's for each separate inhabited space station compartment.	LD-8C -33I		8.22

SYSTEM: 2. Crew System (Page 1 of 6)

TABLE 3.3-2 (cont.)

SYSTEM: 2. Crew System (cont.)		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	**Recommended Safeguards**			
2.1 EVA equipment failure (cont.)	2.1.9 Provide backup emergency communications between EVA personnel and space station.	LD-18E	78	12.26
	2.1.10 Provide visual monitoring capability at a central control console of all EVA personnel, including airlock activities.	LD-11F	78	12.48
	2.1.11 Provide emergency lighting for EVA crew rescue during darkside operations.	LD-80B	1	12.27
	2.1.12 Provide detailed emergency procedures to cope with all foreseeable contingencies that might arise during EVA.	LD-12E	1	12.31
	2.1.13 Design structures and equipment to minimize the possibility of damage to pressure suits and umbilicals.	FT 1.2-C LD-52C	1	5.8
2.2 Food contamination	2.2.1 Provide multiple food storage containers so contamination of one will not affect the others.	LD-31G -59B		1.12
	2.2.2 Provide redundant cooling circuits for food storage containers.	LD-10F -31G		[illegible]
	2.2.3 Monitor water dispenser water potability to preclude contamination of food by bad water.	LD-31G -76K		1.29
	2.2.4 Provide for sterilization of foods and food storage areas.	LD-31G -59B	98	1.13
	2.2.5 Assure complete sealing of food containers to preclude contamination from outside sources.	LD-31G -59B	98	1.12

SYSTEM: 2. Crew System (Page 2 of 6)

TABLE [illegible] ([illegible])

SYSTEM: [illegible] Crew System (cont.)			Analysis Reference	Doc Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
[illegible] Radiation	[illegible].3.1	Compensate for periods of maximum solar activity during long-term missions by providing area of greatest protection from radiation for crew retreat ("storm shelter"). Such area must be self-sufficient so crew can operate spacecraft and live for periods up to the maximum expected duration of hazard. EVA also must be prohibited for longer periods of time during major solar events and for 1 to 2 days during minor solar events.	FT [illegible].2-H LD-30C, D -30E -40C -42D	43 99	9.15
	2.3.2	Provide capability for continuously monitoring radiation, from both the space station and from Earth, to gain advance warning of solar activity. Such capability should be redundant to ensure continuous active operation.	FT 3.4-D LD-10F -18D -40B	43 78	9.17
	2.3.3	Continuously monitor individual crew member radiation dose accumulations.	FT 3.4-G LD-32E	9 78	9.15
	2.3.4	Locate space station equipment, storage tanks, spare parts, supplies, etc., to obtain maximum benefit for radiation shielding.	FT 3.1-M LD-32E -51B	43	9.9
	2.3.5	Provide protection from radiation of a nuclear bomb explosion near the space station orbiting altitude. Alternately, provide for changing orbit to avoid radiation belts.	FT 3.3-J LD-8E -32E	65 99	9.10
	2.3.6	Restrict operation of on-board [illegible] of RF radiation during crew EVA.	LD-3[illegible]E -38C	5	5.[illegible]

SYSTEM: [illegible] Crew System ([illegible])

TABLE 3.3-2 (cont.)

SYSTEM: 2. Crew System (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
2.4 Crew injury or illness	2.4.1 Design space station equipment to minimize dangers to the crew from sharp projections, hot or cold surfaces, excessive acceleration, vibration, noise, electrical current.	LD-27C	20 43 50	5.5
	2.4.2 Provide adequate volume for freedom of crew member movement.	LD-48B, E	26 50	12.51
	2.4.3 Provide adequate lighting, including emergency lights, for all areas in which crew members may be required to perform tasks or maintenance, including EVA.	LD-10G -48F, H		12.43
	2.4.4 Display critical caution and warning visual/audible alarms in all inhabited compartments. Crew members in normally uninhabited areas or on EVA should be in constant communication with a crew member at a control console.	LD-18D -48H, I	50	12.22 12.26 12.48
	2.4.5 Make readily available medical supplies and medical skills on-board the space station to handle any expected event. Medical consultation with an Earth station should be available at all times, either directly or by relay satellite.	LD-22D -23D -69J -70J	26 68	7.16
	2.4.6 Provide adequate restraints, tethers or aids to assist crew movement throughout interior and exterior of space station, and for handling equipment with a large mass or potentially high momentum.	LD-13C, F -32C	26 43 50	5.10

SYSTEM: 2. Crew System (Page 4 of 6)

TABLE 3.5-1 (cont.)

SYSTEM: 2. Crew System (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguard			
2.4 Crew injury or illness (cont.)	2.4.7	Design, or provide protection for, equipment located on exterior surface of space station (e.g., solar panels, antennas) so it does not constitute a hazard to EVA personnel and to rendezvous and docking operations.	FT 1.2-G LD-52C	43	5.7 5.8
	2.4.8	Provide required support capability to permit EVA crew members to perform tasks under extreme variations in light contrasts, light intensities, and temperatures.	LD-46B -78G	43	5.8 12.27 12.45
	2.4.9	Design space station systems to minimize requirements for EVA through use of redundancy, high reliability components, backup modes of operation. In addition, these systems and components should be designed for easy replacement by a pressure suited crewman or a remote manipulator unit in case replacement does become necessary.	LD-10G -25G	80	12.46
	2.4.10	Avoid operation of equipment that would endanger crew EVA.	LD-32B, C	1	5.5
	2.4.11	Provide protection against suffocation or drowning in a zero-g whole-body crew shower concept.	LD-15E	108	9.6
2.5 Inadequate maintenance capability	2.5.1	Provide replacement parts to cover the maximum expected failures between resupply missions.	LD-9G -18E	43 80	12.56

SYSTEM: 2. Crew System (Page 5 of 6)

TABLE 3.3-2 (cont.)

SYSTEM: 2. Crew System (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
2.5 Inadequate maintenance capability (cont.)	2.5.2 Provide redundancy for critical system components to permit continuous operation during replacement time of failed component.	LD-10F	38 43	*
	2.5.3 Provide auxiliary maintenance equipment, including spare parts for this equipment, to handle possible failures.	LD-18E -47E	43 51	12.45
	2.5.4 Provide maintenance instructions and rapid access to these instructions.	LD-9F -18D	43 51	12.45
	2.5.5 Provide inventory control of all spare parts to permit efficient determination and resupply of required spares.	LD-18E	20 43	12.56
	2.5.6 Provide access through space-to-Earth communications to qualified technicians for all space station systems.	LD-50E	26 43	12.45
	2.5.7 Design replaceable equipment so it is physically impossible to be installed improperly.	LD-10D	102	12.55
	2.5.8 Provide fault isolation capability to allow rapid detection of faulty components.	LD-10G	20 43	12.45
	*A number of guidelines were written for each of the applicable subsystems regarding redundancy recommendations. Examples are: 1.14, 5.4, 8.13, 8.22, 10.26, 11.3, 12.15 and 12.31.			

SYSTEM: 2. Crew System (Page 6 of 6)

TABLE 3.3-1

SYSTEM: 3. Electrical Power System		Analysis Reference	Doc. Ref.	Applic. Guidelines
Potential Hazard	**Recommended Safeguards**			
3.1 Fire, smoke, toxic products	3.1.1 Incorporate protective devices to limit current to circuits or equipment which are carrying excessive current.	FT 2.5-D LD-8D	22	10.14
	3.1.2 Provide adequate venting of batteries to prevent over-pressure and possibility of battery gas products from contaminating pressurized compartment.	LD-8F -61D	50 98	1.2
	3.1.3 Provide adequate cooling of power sources to prevent overheating. Cooling provisions should be redundant if cooling equipment failure cannot be tolerated.	FT 2.3-D LD-8D -[illegible]D	90	10.9
	3.1.4 Locate power-generating and distribution equipment which are potential sources of fire in unpressurized areas of the space station wherever practical.	FT 2.1-B LD-16D -32D	22	10.6
	3.1.5 Provide emergency shut-down and heat dissipation capability in case of failure of cooling system for nuclear power sources.	LD-57D -58D		9.7
	3.1.6 Adequately shield equipment with high speed rotating components to prevent wheel rupture from damaging other equipment.	LD-[illegible]C, D -[illegible]7D		5.1[illegible]
	3.1.7 Place detectors in the vicinity of potential sources of fire, smoke, toxic odors and flammable gases to initiate audio/visual alarms in all inhabited areas.	FT 2.10-D LD-8D, H -45E	2[illegible]	12.3[illegible]

SYSTEM: 3. Electrical Power System (Page [illegible] of 4)

TABLE 3.3-3 (cont.)

SYSTEM: 3. Electrical Power System (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guidelines
3.1 Fire, smoke, toxic products (cont.)	3.1.8 Provide fire extinguishing equipment which can be automatically initiated, or where it will be readily accessible and can be manually controlled, as the situation warrants. Adequate precautions should be taken to ensure that the correct extinguishing system is used for a particular fire.	FT 2.7-B LD-8D -18E -47E	26 55 78	10.7 10.23
	3.1.9 Route power distribution wires so that any fire damage from a fault will have a minimal effect on other power distribution wires.	FT 2.5-D	51	4.14
	3.1.10 Locate smoke detectors in all primary ventilation ducts.	FT 2.10-D LD-8H -76J		1.1
	3.1.11 Provide for (a) automatic shut-down of ventilating equipment and O_2 supply upon detection of fire and/or (b) other effective methods for control of fires.	FT 2.9-B LD-8D -15K	50 78 108	10.7
	3.1.12 Provide for controlled dumping of cabin air to prevent buildup of smoke or toxic odors.	FT 2.17-C LD-42H -45B	50	1.5
	3.1.13 Establish emergency procedures, and regularly train the crew in these procedures, to be followed in the event of a fire, either in pressurized or unpressurized areas.	FT 2.7-I LD-4C	9	12.28
	3.1.14 Prohibit smoking or the use of open flames in any pressurized areas of the space station.	FT 2.3-J LD-16D	50	10.14

SYSTEM: 3. Electrical Power System (Page 2 of 4)

TABLE 3.3-4 (cont.)

SYSTEM: 3. Electrical Power System (cont.)		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	Recommended Safeguards			
3.1 Fire, smoke, toxic products (cont.)	3.1.15 Provide separately pressurizable compartments in the space station which can be sealed off and vented to vacuum in case of fire or smoke.	FT [illegible]-I	26 30	[illegible]
	3.1.16 Design electrical equipment to be explosion-proof.	FT [illegible].11-E	8	6.2
	3.1.17 See Table 3.3-4 for safeguards pertaining to fluid leakage in the EC/LSS.	--	--	--
3.2 Loss of electrical power	3.2.1 Provide multiple power sources so that a single failure will not jeopardize crew safety.	LD-[illegible]F	9	4.11
	3.2.2 Provide an independent power source for emergency use only and capable of supplying minimum equipment requirements for crew safety.	LD-6B		12.38
	3.2.3 Provide multiple power distribution paths so electrical equipment can be connected to more than one power source.	LD-[illegible]F	92	[illegible]
	3.2.4 Provide capability to monitor critical parameters of each power source.	LD-9E -15D		4.10
	3.2.5 Provide automatic shut-down or power source isolation when operating needs exceed normal limits.	LD-6B		4.10

SYSTEM: 3. Electrical Power System (Page 3 of 4)

TABLE 3.3-3 (cont.)

SYSTEM: 3. Electrical Power System (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
3.2 Loss of electrical power source (cont.)	3.2.6	See Table 3.3-1, Item 1.4.1, for safeguard pertaining to critical computer functions.	--	--	--
3.3 Power source radiation	3.3.1	Locate power source so that maximum structural and equipment weight is between power source and inhabited areas of the space station.	FT 3.5-H LD-57B		9.5
	3.3.2	Locate power source and provide adequate shielding to protect EVA personnel, rendezvous and docking operations with other satellites or vehicles, and radiation-sensitive equipment.	FT 3.1-M LD-57F		9.5
	3.3.3	Provide alternate method for cooling power source in case of failure of primary cooling system.	FT 2.15-G LD-8D		10.5
	3.3.4	Provide means for additional shielding protection from radiation when personnel are performing EVA.	FT 3.5-C LD-8E		9.18
	3.3.5	Provide means for emergency shut-down of power source in event of system failure which cannot be controlled by other means.	LD-8E -58D		9.7
	3.3.6	Provide area within space station which has maximum radiation protection for personnel to use if radiation becomes excessive.	FT 3.2-H LD-8E		9.16
	3.3.7	Design power source support structure and radiation shield to be capable of withstanding micrometeoroid damage and space station maneuvers.	FT 3.5-H LD-57D -57E	65	9.5

SYSTEM: 3. Electrical Power System (Page 4 of 4)

TABLE 3.3-4

SYSTEM: 4. Environmental Control/Life Support			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
4.1 Loss of O_2	4.1.1	Monitor O_2 quantity and provide visual alarm when usage rate exceeds certain limits or quantity decreases to specified level.	FT 1.1-D LD-15K -48H	9 68	8.12
	4.1.2	Provide shut-off valves to isolate possible sources of O_2 leakage.	FT 1.1-D LD-15K		8.11
	4.1.3	Provide multiple O_2 storage tanks so leakage or failure of one will not critically deplete amount of O_2.	FT 1.1-D LD-33I	50 108	8.14
	4.1.4	Provide redundancy of components which control and regulate O_2 pressure of cabin atmosphere.	FT 1.4-C LD-44C	22 80	8.13
	4.1.5	Monitor cabin O_2 level and provide visual/audible alarm when O_2 pressure is not within certain limits.	FT 1.1-E LD-44C -48H, I	9 68 103	8.30
	4.1.6	For O_2 systems of 3000 psi or higher, install valves which are slow opening and closing to minimize the possibility of ignition of contaminants.	LD-16D	103	10.24
	4.1.7	Incorporate protective devices in primary battery circuit to prevent reversing polarity on water electrolysis unit cells which could result in an explosive mixture of H_2 and O_2.	FT 2.7-U	41	6.13
	4.1.8	Provide capability for manually controlling O_2 usage.	FT 1.1-D LD-48F		8.15

SYSTEM: 4. Environmental Control/Life Support (Page 1 of 9)

TABLE 3.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
4.2 Loss of cabin pressure	4.2.1 Monitor total cabin pressure and provide visual/audible alarm when pressure deviates beyond certain limits.	LD-8C -24I -48H, I	9	3.24
	4.2.2 Monitor rate of change in total cabin pressure and provide visual/audible alarm when pressure rate of change exceeds a certain limit.	LD-8C -24I -48H, I	3 9	3.24
	4.2.3 Provide sensors to detect leakage of cabin pressure through seals and pressure shell.	FT 1.1-J LD-8C	50	8.17
	4.2.4 Provide means for bypassing or inactivating relief valves which could be the cause of cabin pressure loss.	FT 1.4-C LD-8C		8.18
	4.2.5 Provide capability for continuous control of cabin pressure.	FT 1.4-C LD-42H	55	8.5
	4.2.6 Design for accessibility and include on-board capability to repair pressure wall damage or to replace failed seals which are source of cabin pressure leakage.	FT 1.1-J LD-48B, F	38	3.17
	4.2.7 Provide capability for individual environmental control of more than one separately pressurizable spacecraft compartment so that pressure loss in one compartment will not incapacitate entire spacecraft.	FT 1.1-C LD-34C	22 26 92	 8.9 12.13
	4.2.8 Provide automatic closure of intercompartment hatches when cabin pressure decreases below a specified limit.	FT 1.1-E LD-8C -12E	26	3.4

SYSTEM: 4. Environmental Control/Life Support (Page 2 of 9)

TABLE 3.3.4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)		Analysis Reference	Doc. Ref.	Applic. Guidelines
Potential Hazard	**Recommended Safeguards**			
4.2 Loss of cabin pressure (cont.)	4.2.9 Provide readily available emergency life support equipment for use during or after rapid loss of pressure.	FT 1.5-C LD-8C -48C		3.7
	4.2.10 Design and install components which are vented to space to be replaceable without requiring cabin depressurization.	FT 1.4-F LD-48F		3.[illegible]
	4.2.11 Design equipment located in pressurized compartments to withstand rapid decompression of the space station.	FT 1.5-E LD-9B	51 78	3.3
	4.2.12 Provide separate O_2 supply for emergency pressurizations.	FT 1.5-C LD-33I	9 38	[illegible]
	4.2.13 Design evacuation system so that cabin pressure is not vented to space through compartments or outlets used to vent other fluids.	LD-15K -16C	51 90	[illegible]
4.3 Excessive CO_2	4.3.1 Monitor CO_2 partial pressure and provide visual/audible alarm when pCO_2 increases above a certain limit.	LD-45B -48H, I -76J	9 68	[illegible]
	4.3.2 Provide redundant CO_2 removal systems so continuous capability is available even if failure of one system does occur.	LD-8H -10F -45B	55 80	1.7
	4.3.3 Provide capability for manually controlling operation of the equipment used for CO_2 removal.	LD-8H -45B		1.7
	4.3.4 Monitor atmosphere relative humidity and provide visual warning when specified limits are exceeded.	LD-18D -48H	9 68	1.27

SYSTEM: 4. Environmental Control/Life Support (Page 3 of 9)

TABLE 3.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guidelines
4.3 Excessive CO_2 (cont.)	4.3.5 Assure that CO_2 control equipment involving very high temperatures and/or carbon or other contaminant products conforms with special maintenance considerations.	LD-10G -32B -48F -61E	108	10 1
4.4 Fluid leakage	4.4.1 Provide shut-off valves to isolate plumbing or equipment which is susceptible to leakage.	LD-6B	103 108	1.10
	4.4.2 Use fluids which will not be harmful to the crew in the event leaking fluids contaminate the cabin atmosphere.	LD-16H	51	1.23
	4.4.3 Use fluids in inhabited areas which are non-toxic and non-flammable.	LD-16D, H	90	1.23
	4.4.4 Provide detectors which will activate visual alarms when atmosphere fluid contaminants exceed prescribed limits.	LD-8H -44B -48H	68 89	1.24
	4.4.5 Design components and plumbing in fluid systems so replacement can be made with no fluid loss.	LD-10C -61D	108	1.21
	4.4.6 Design fluid lines to have a minimum of connections.	LD-10G	103 108	1.22
	4.4.7 Provide sensors in fluid tanks which use a pressurant, and have a separation device to prevent mixing of the fluid and pressurant, to detect a leakage or rupture of the separation device. Provision should also be made for isolating the contaminated systems and subsequent purging the contaminants.	LD-6B	108	1.25

SYSTEM: 4. Environmental Control/Life Support (Page 4 of 9)

TABLE 5.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
4.4 Fluid leakage (cont.)	4.4.8	Provide automatic relief valves, or other protective devices, for any pressure volume that can be confined or isolated by system valving.	LD-13D -60D -61D	90 103	3.15
	4.4.9	Vent pressure relief devices for all fluid volumes to safe areas or equipment, and away from inhabited areas.	LD-60D -61D	78	3.22
	4.4.10	Provide fluid quantity displays to permit monitoring of fluid usage.	LD-9E		12.34
	4.4.11	Avoid locating pressure systems in proximity to other sources of high energy such as heat, voltage or leakage from other systems; or provide adequate shielding.	FT 1.12-D LD-16F -61D	102	6.7
	4.4.12	Provide restrictions in pressurized gas supplies which will limit gas flow, resulting from a plumbing failure, to a rate which can be handled by the available venting system.	LD-15C -16F	51	3.16
	4.4.13	Provide means for collecting and/or containing loose fluids or debris resulting from maintenance or equipment operation.	LD-32B -60D -61D -65D	80 103	1.9
4.5 Atmosphere contamination	4.5.1	Monitor contaminant levels of atmosphere and provide visual/audible alarm when contaminants exceed specified levels.	LD-18D -44B -48H, I	68 78 89	1.24
	4.5.2	Monitor flow of air-circulating equipment and provide visual alarm if flow decreases below specified levels.	LD-15K -33E -48H	55	8.1

SYSTEM: 4. Environmental Control/Life Support (Page 5 of 6)

TABLE 5.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	**Recommended Safeguards**			
4.5 Atmosphere contamination (cont.)	4.5.3 Provide air circulation which will preclude the possibility of stagnant air pockets existing within inhabited areas.	LD-44B, C -45B		[illegible]
	4.5.4 Provide procedures for controlling and eliminating atmosphere contamination (e.g., cabin depressurization, controlled leakage of air) which is in excess of the contaminant control system's capability.	FT 2.17-C LD-8H -45B	98	1.5
	4.5.5 Provide redundancy for contaminant control and detection equipment.	LD-10F	30	1.4 12.40
	4.5.6 Provide redundancy for air circulation equipment.	LD-10F	55,80	8.1
	4.5.7 Design all filters, screens or other devices for collecting contaminants or waste products so they can be easily replaced without releasing contaminants into the atmosphere.	LD-10G -32B -60E -61E	43 108	1.3
	4.5.8 Provide individual emergency sources of O_2 for each crewman in event contamination becomes excessive.	LD-44B, C	22 26	8.7
	4.5.9 Provide for containing, venting or eliminating odors and bacteria or waste products.	LD-21B -45B	50	1.28
	4.5.10 Monitor air composition in air ducts immediately downstream of potential major sources of contamination and provide automatic airflow cut-off if excessive contamination is detected.	LD-8H -18D -44B -45B		1.1

SYSTEM: 4. Environmental Control/Life Support (Page 6 of 9)

TABLE [illegible] (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
4.5 Atmosphere contamination (cont.)	4.5.11 Incorporate interlocks which will preclude the use of critical equipment that is not operating within acceptable limits.	LD-6B -9C	41	8.10
	4.5.12 Provide protection for cabin fans from floating objects and debris.	LD-43F -45B	90	8.1
	4.5.13 Avoid the use of mercury aboard the spacecraft.	LD-59B, F -61B, D	90	1.19
	4.5.14 See Table 3.3-3, Part 3.1, for safeguards pertaining to fire, smoke and toxic products.	--	--	--
4.6 Loss of thermal control	4.6.1 Monitor temperatures of atmosphere and thermal control fluids at critical points in the system and provide visual/audible alarm if temperature exceeds specified limits.	FT 2.9-B LD-8D -18D -48H, I	9 90	10.27
	4.6.2 Provide redundancy for critical thermal control equipment, in particular for that equipment located in uninhabited areas.	LD-8D -10F	80 108	10.26
	4.6.3 Provide capability to automatically shut down equipment which would be damaged by out-of-tolerance temperatures.	FT 2.8-G LD-8D		10.22
	4.6.4 Provide alternate or redundant thermal control for equipment with critical thermal control requirements.	LD-8D -10F	80 108	10.22
	4.6.5 Provide capability for manual operation of valves which control cabin and equipment temperature.	LD-46D		10.18

SYSTEM: 4. Environmental Control/Life Support (Page 7 of 9)

TABLE 3.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
4.7 Water contamination	4.7.1	Provide multiple water storage tanks so contamination of one tank will not critically affect the water supply.	LD-31G -59B	50	8.33
	4.7.2	Monitor water composition and provide visual warning when contamination exceeds specified limits.	LD-48H -59B	55 108	1.29
	4.7.3	Provide means for reclaiming or disposing of contaminated water and restoring equipment to within acceptable cleanliness criteria.	LD-30D -76C	108	8.31
	4.7.4	Locate water tanks so possibility of contamination from other spacecraft equipment is minimized.	LD-21B -76C	98	1.32
	4.7.5	Provide protective devices as necessary to prevent contaminated water in one tank, or set of equipment, from entering other tanks or equipment.	LD-9C -21B -76C	90 98	1.31
	4.7.6	Provide means for keeping on-board water supplies sterile.	LD-21D -30D	108	1.30
	4.7.7	Provide redundancy for potable water sterilization system.	LD-10F -30D	80	8.32
4.8 Loss of suit loop	4.8.1	Provide redundancy for critical suit loop components.	FT 1.1-F LD-10F	9 80	8.26
	4.8.2	Provide multiple outlets in suit loop.	LD-45B	55	8.28
	4.8.3	Provide capability to easily isolate and replace faulty components of the suit loop.	LD-10G -48F		8.25

SYSTEM: 4. Environmental Control, Life Support (Page 8 of 9)

TABLE 4.3-4 (cont.)

SYSTEM: 4. Environmental Control/Life Support (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
4.8 Loss of suit loop (cont.)	4.8.4 Provide for periodic check-out of suit loop operation.	FT 1.1-F,G LD-10G	8	8.24
	4.8.5 Provide for autonomous operation of the suit loop to permit isolating the suit loop from the compartment EC/LSS.	LD-33I -34I	55	8.4
	4.8.6 Provide for monitoring suit loop pressure while suit loop is in use.	FT 1.1-F LD-44E		8.29
	4.8.7 Provide capability for manual operation of valves which control suit loop operation.	FT 1.1-F LD-18E -27E	27	8.27

SYSTEM: 4. Environmental Control/Life Support (Page 9 of 9)

TABLE 4.3-5

SYSTEM: 5. Stability and Control		Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard	**Recommended Safeguards**			
5.1 Loss of attitude control	5.1.1 Provide redundancy for all components located outside pressurized areas.	LD-10F -14B	22	11.3
	5.1.2 Provide means for stopping propellant flow to failed open thrusters.	LD-11E -35E	9 22	11.10
	5.1.3 In propellant distribution system incorporate automatic shut-down of propellant flow to operating thruster(s) if spacecraft angular rates or thruster duration exceeds certain limits.	LD-17E -35E		11.1 11.10
	5.1.4 Provide capability for on-board crew to manually activate and control primary and redundant thrusters.	LD-17E -18E -35E	78	11.8
	5.1.5 Provide capability for either ground station or flight crew to initiate operation of an on-board automatic system for activating and controlling thrusters to restore spacecraft stability.	LD-4D -17E -18E		11.2
	5.1.6 Provide replacement capability for components of control moment gyros (if used).	LD-10G -18E	48 80	11.4
	5.1.7 Provide automatic override of attitude control to prevent spacecraft closure rates during docking maneuvers from exceeding a certain limit.	FT 1.7-K LD-12E -35B		5.3
	5.1.8 Provide visual/audible alarm if spacecraft angular rate exceeds a certain limit.	LD-11E -48H, I	3	11.1
	5.1.9 Design for and maximize commonality of electronic components with logistics vehicles and independent modules, where practical.	LD-9D		12.57

SYSTEM: 5. Stability and Control (Page 1 of 3)

TABLE 5.[illegible]-[illegible] (cont.)

SYSTEM: 5. Stability and Control (cont.)				
Potential Hazard	Recommended Safeguards	Analysis Reference	Doc. Ref.	Applic. Guideline
5.1 Loss of attitude control (cont.)	5.1.10 Provide interlocks to prevent simultaneous manual and automatic operation of the stability and control system.	LD-9C -11E -53D		11.7
	5.1.11 Provide multiple propellant tanks with capability to feed any thruster from any tank.	LD-10F -11E		11.12
	5.1.12 Provide redundant attitude indicator displays.	LD-10F	9	12.[illegible]
	5.1.13 Monitor temperature of thruster assemblies and/or provide visual alarm if temperature exceeds specified limits.	LD-8D -18D -48H, I		10.3[illegible]
5.2 Propellant leakage	5.2.1 Provide shut-off valves to isolate plumbing or equipment which is susceptible to leakage.	LD-61D	103	1.10
	5.2.2 Locate propellant storage and distribution system components for toxic or potentially flammable fluids in uninhabited areas, or provide appropriate shielding.	FT 2.6-G LD-8D -59D -61D	50 98	10.20
	5.2.3 Locate fuel and oxidizer supply systems to minimize possibility of their combining if leakage does occur.	FT 2.6-D,F LD-16D	9 103	10.20
	5.2.4 Locate equipment (including electrical wiring), which could become contaminated or damaged by propellants, so as to preclude the equipment from coming in contact with leaking propellants, or provide suitable protection for the equipment.	LD-9C -32B	103	1.8

SYSTEM: 5. Stability and Control (Page 2 of 3)

TABLE 3.3-5 (cont.)

SYSTEM: 5. Stability and Control (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
5.2 Propellant leakage (cont.)	5.2.5	Provide leak detectors which would activate a visual alarm at the command and control console.	LD-8H -48H		12.52
	5.2.6	Provide displays to monitor propellant usage and quantity of propellant remaining.	LD-9E, G -48H	90	12.53
5.3 Propellant tank rupture	5.3.1	Separate propellant tanks to minimize damage to other tanks if one ruptures, or provide adequate shielding.	LD-17E		6.10
	5.3.2	Provide adequate protection from meteoroid penetrations.	FT 1.3-G LD-17E		6.10
	5.3.3	Locate tanks, or provide protection. to preclude damaging tanks during docking operations and cargo handling.	FT 1.7-K LD-12E -35B		6.10
	5.3.4	Provide redundant relief valves with separate vents to ensure against tank rupture from overpressure.	LD-8F -10F -13D	80 103	6.9
5.4 Exhaust plume	5.4.1	Design spacecraft configuration so that relation of thruster location and orientation to external equipment avoids exhaust impingement on equipment (e.g., solar panels, antennas).	LD-9D		10.28
	5.4.2	Provide design safeguards and/or procedures to preclude operation of thrusters whenever personnel are involved in EVA.	LD-8D -9E -32		10.29 12.50

SYSTEM: 5. Stability and Control (Page 3 of 3)

TABLE 3.3-6

SYSTEM: 6. Structures/Mechanical			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
6.1	No airlock capability	6.1.1 Provide redundant pressurization capability for airlock.	LD-8C -10F		12.3
		6.1.2 Provide more than one airlock for space station.	LD-80B		12.4
		6.1.3 Provide capability to monitor O_2 usage during airlock pressurization.	LD-18D -42D		8.2
		6.1.4 Provide alternate methods of opening/closing airlock hatches.	LD-8C -80B		12.2
		6.1.5 Provide capability for easy replacement of seals.	FT 1.1-L,M LD-10G		3.10
		6.1.6 Provide multiple O_2 connections inside airlock for pressure suits.	LD-33I		8.3
6.2	Docking accident	6.2.1 Provide multiple docking ports.	FT 1.7-K LD-80B		5.5
		6.2.2 Provide capability to isolate cabin areas in vicinity of docking port to minimize atmosphere loss.	FT 1.3-C LD-8C		5.2
		6.2.3 Provide redundant docking lights and multiple power sources for the lights.	FT 1.7-K LD-46B	27	5.4
		6.2.4 See Table 3.3-5, Part 5.1, for safeguards pertaining to loss of attitude control.	--	--	--
6.3	Cannot transfer resupply cargo	6.3.1 Provide multiple docking ports.	FT 1.7-K LD-80B		5.5
		6.3.2 Provide alternate methods for transferring resupply cargo.	FT 1.7-G LD-48E		12.9

SYSTEM: 6. Structures/Mechanical (Page 1 of 2)

TABLE 3.3-6 (cont.)

SYSTEM: 6. Structures/Mechanical (cont.)			Analysis Reference	Doc. Ref.	Applic. Guideline
Potential Hazard		Recommended Safeguards			
6.4 Structural damage	6.4.1	Design pressure shell to be capable of withstanding maximum probable micrometeoroid impacts, and of withstanding continual skin erosion over a ten-year mission.	FT 1.1-J LD-16C -52B	65 78	3.19
	6.4.2	Design windows to permit replacement of eroded or damaged surfaces without degrading pressure or structural integrity of spacecraft hull.	LD-9G -16C -48F	65	2.4
	6.4.3	Provide adequate restraints, tethers and space station free volume to permit handling of large mass equipment without damaging other equipment or crew members.	LD-9E -18E -48E	26	5.10
	6.4.4	Provide capability to detect and locate micrometeoroid punctures of pressurized compartments.	LD-18E -34C	78	8.17

SYSTEM: 6. Structures/Mechanical (Page 2 of 2)

4.0 REFERENCES

The references listed on the following pages were used while performing the analyses described in this document. Reference numbers match those of the master reference list given in Document D2-113070-5, Crew Safety Guidelines.

No.	Title	Report No.	Source	Date	Contract No.	Cl.
1	AAP Crew Operations--Crew Safety Analysis, Cluster Mission AAP Flight #2, Vehicle AS 209 (Including experiment hazards)	ED-2002-24, Revision A	Martin	2/10/67	NAS8-21004	U
3	AAP Payload Integration--Orbital Workshop Crew Hazard Analysis	ED-2002-284, Revision C	Martin	7/31/68	NAS8-24000	U
5	AAP Payload Integration--RF Radiation Exposure During EVA Film Recovery	ED-2002-442	Martin	4/15/68	NAS8-24000	U
8	Apollo Logistics Support System (ALSS) Payloads--MOLAB Reliability and Crew Safety	D2-83212-1	Boeing	6/65	NAS8-11411	U
9	Apollo Operations Handbook, Command and Service Modules--Operational Procedures (Apollo 9, CSM 104)	SM2A-03-SC104-(2), Volume 2	NASA/MSC	1/20/69	NAS9-150	U
10	Apollo Spacecraft Integrated System Safety Assessment CSM-104/LM-3, Mission "D"	D2-118112-3 (Volumes I and II), D2-113112-3A (Volume I, Revision A)	Boeing	1/14/69	NASw-1650	U
18	Contingency Planning for Space-Flight Emergencies	Memorandum RM-5200-NASA	S.H. Dole, et al.-Rand Corp., Santa Monica	1/67	NASr-21(13)	U
20	Design/Maintainability Trades	D2-113551-1	Boeing	4/67	---	U
22	Early Orbital Space Station (EOSS), Technical Report	DAC-56550	McDonnell-Douglas	11/67	---	U
26	Factors Affecting the Interior Design of Crew Compartments for Long-Duration Space Flight	MSC Internal Note #68-ET-16	NASA/MSC	9/15/67	---	U

No.	Title	Report No.	Source	Date	Contract No.	[illegible]
[illegible]	Failure Modes and Effects Analysis for the IM-- Vehicle (Mission Oriented)	LED [illegible], Volume I	Grumman	[illegible]	NAS9-[illegible]	
38	Intermediate Workshop Study, Modular Approach	MSC-EA-R-68-1, Volume 1	NASA/MSC	[illegible]	---	U
41	Life Support Systems for Space Flights of Extended Time Periods	NASA CR-614	General Dynamics	[illegible]	NAS1-2934	
42	Maintainability of Manned Spacecraft for Long-Duration Flights--Summary Report	D2-113204-1, Volume I	Boeing	[illegible]	NAS2-[illegible]	U
43	Maintainability of Manned Spacecraft for Long-Duration Flights--Technical Report	D2-113204-2, Volume II	Boeing	7/67	NAS2-[illegible]	U
44	Maintainability of Manned Spacecraft for Long-Duration Flights--Work Data	D2-113204-3, Volume III	Boeing	7/67	NAS2-[illegible]	U
46	Manned Orbital Research Laboratory (MORL) Study--Environmental Control/Life Support System	SM-46085	Douglas	9/64	NAS1-[illegible]	U
47	Manned Orbital Research Laboratory (MORL) Study--Safety, Reliability and Maintainability	SM-44615	Douglas	9/62	NAS1-[illegible]	S
48	Manned Orbital Research Laboratory (MORL) Study--Stabilization and Control System	SM-46086	Douglas	9/64	NAS1-[illegible]	
49	Manned Orbital Research Laboratory (MORL) Study--System Improvement Study--Stabilization and Control	SM-48817	Douglas	12/65	NAS1-[illegible]	U
[illegible]	Manned Orbital Research Laboratory (MORL) Study--Systems Analysis; Flight Crew	SM-46075	Douglas	9/64	NAS1-3612	U
[illegible]	Manned Spacecraft Criteria and Standards	MSCM 8080	NASA/MSC	1/68	---	U

No.	Title	Report No.	Source	Date	Contract No.	Cl.
55	Mars Landing and Reconnaissance Mission Environmental Control and Life Support System Study	SLS 414-3	Hamilton Standard	3/64	NAS9-1701	U
65	Operations and Logistics Study of a Manned Orbital Space Station	LR 17366	Lockheed	12/63	NAS9-1422	C
68	Preliminary Terminal Data for Earth Orbiting Space Station--Standards and Criteria	MSC-EA-R-66-1, Volume II	NASA/MSC	11/7/66	---	U
[illegible]	Report on the Optimization of the Manned Orbital Research Laboratory (MORL) System Concept--Summary Report	SM-46[illegible]1	Douglas	9/64	NAS1-3612	U
[illegible]	Risk of Bends During Apollo Operations at 3.[illegible] psia, Case 32[illegible]	B69-13028	Bellcom, Inc.	3/12/69	---	U
[illegible]	Safety Requirements for Man-Rating Space Systems (Draft)	---	NASA/Headquarters	11/8/68	---	U
[illegible]	Saturn V Single Launch Space Station and Observatory Facility, Earth Orbital Station Utilization	LL-113538-1	Boeing	11/67	NAS9-6816	U
9[illegible]	Space Design Data	D2-114000-1	Boeing	1/69	---	U
9[illegible]	Space Flight Emergencies and Space Flight Safety---A Survey	[illegible]-1730	Staff Study for the Subcommittee on NASA Oversight, of the Committee on Science & Astronautics, U.S. House of Representatives, 90th Congress, U.S. Government Printing Office, Washington	1967	---	U

No.	Title	Report No.	Source	Date	Contract No.	[illegible]
91	Space Flight Hazard Catalog (Preliminary)	---	NASA/MSC; Flight Safety Office (F.J. Bailey)	1968	---	U
92	Space Station Program Definition Study (Phase B)--Statement of Work	9-4-7895	NASA/Headquarters	4/14/69	---	U
96	Study for Basic Subsystem Module Preliminary Definition	GDC-DAB67-003	General Dynamics	10/67	NAS9-6[illegible]96	U
97	Study of a Rotating Manned Orbital Space Station--Human Factors	LR 17502, Volume 6	Lockheed	3/64	NAS9-1[illegible]5	U
98	Study of Manned Space Flight Emergency Concepts--Appendices	ATR-68(7080)-2 Volume II	Aerospace Corp.	4/68	NASW-1561	U
99	Study of Radiation Hazards to Man on Extended Missions (II)	D2-114299-1	Boeing	3/25/69	NASw-1362	U
102	System Safety Handbook	NAS TMX-53563	NASA/MSFC	12/68	---	U
103	System Safety Requirements for Aerospace Vehicles and Ground Equipment	D2-113069-1	Boeing	4/8/69	---	U
108	Trade-Off Study and Conceptual Designs of Regenerative Advanced Integrated Life Support Systems (AILSS)	---	Hamilton-Standard	7/69	NAS1-7905	U
111	Voyager Failure Modes and Effects Analysis	D2-82724-2	Boeing	8/65	JPL 951111	U
115	Earth Orbital Laboratory Environmental Control and Life Support System	---	W.W. Guy--NASA/MSC	9/66	---	U

PRECEDING PAGE BLANK NOT FILMED.

APPENDIX A

PHASE I FAILURE, SAFETY AND MAINTENANCE ANALYSIS DATA SHEETS

The data sheets included herein are those which were generated during the Phase I part of the study as described in Section 2.0. The following provides an explanation of the data entries used in the analysis:

a. Nomenclature---The top entry on each sheet identifies the spacecraft system or subsystem being analyzed. Subsequent entries on the sheet identify the individual components or assemblies which were considered in the analysis. The component list is based on the Saturn V Single Launch Space Station (SVSLSS) study.

b. Quantity---Identifies the number of units of the particular component which are in the basic system as specified in the SVSLSS study.

c. Mod. Loc.---The appropriate module column is marked to identify the location of the component within or on the spacecraft. A "U" or "L" in the core or laboratory column signifies that the component is located in the upper or lower deck of that module. A "B" means the component is located in both decks. "External" indicates the item is located outside of the spacecraft. Location headings may differ and require expansion for analyses made of other specific spacecraft configurations.

d. Critical Failure Mode---A check is made in the appropriate column(s) to identify the critical failure mode(s) of the particular component.

e. Potential Hazard Effect---Lists the potential hazards and/or potential effects that could result from the most critical failure of the component.

f. Hazard Category---Entries in this column are estimates of the worst-case situation that could result if the condition were allowed to continue without any corrective action. The hazard categories are defined as follows:

I ---Any hazard that could result in immediate loss or serious injury to the crew.

II ---Any hazard that could result in continuous emergency operation or cause major damage to the spacecraft.

III---Any hazard that could degrade the mission.

IV ---A nuisance hazard.

g. Safety Provisions---Identifies those safety provisions that are known to be available in the baseline system as well as those that it is felt should be made available.

h. Redundancy Recom.---A check indicates that designed-in redundancy is recommended for this component because of its criticality to the system, accessibility problems, or other factors.

i. Detection Method---A check in the appropriate column(s) indicates which detection method(s) is or should be provided to show that a system failure or degradation has occurred which could have been caused by this component. The detection method may or may not specifically indicate that this particular component has failed.

j. Maintenance Action/Time---A check under "Repair," "Replace" and/or "Service" indicates the type(s) of maintenance expected for this component. The "MTTR" (mean-time-to-restore) entry is an estimate of the mean elapsed time, in hours, required to restore the system to its expected operating condition after a failure of this component has been identified. The figure includes diagnosis, isolation, repair and check-out time increments. Although no entries were made in the "Maximum Downtime" column due to Phase I termination, the column has been retained as a reminder for its inclusion in the event a similar analysis is performed at a later date. Maximum downtime is the maximum elapsed time in hours which could be tolerated before a failure of the component would result in a Category II hazard condition, assuming that there were no safety provisions in the system and that no corrective action was taken.

k. Maint. Constr.---A check is placed in the appropriate column designating a significant constraint on maintenance actions. "EVA/Pressure-Suit" indicates that Extra-Vehicular Activity (EVA) or pressure-suited crew members inside the spacecraft will be required to perform the maintenance function. "Accessibility" means that difficulty may be experienced in gaining access to this component to perform the maintenance action. "Special Tools" and/or "Special Procedures" indicate that these may be required to perform the maintenance action. A small letter entered in a column refers to a similarly coded note given in the "Remarks" column.

l. G.L. Req'd---A check is made in the appropriate column(s) to indicate if "Safety Procedures*," "Emergency Procedures*," or "Safety Design*" Guidelines should be provided to preclude a hazardous condition from occurring; or to contain a condition, caused by failure of the component under review, to keep that condition from developing into a hazardous situation.

*These terms pertain to Phase I of the Safety Study, for which this analysis was conducted. During Phase II, only the single category of "Crew Safety" Guidelines was considered.

m. Crew Skills---Each check indicates that one crew member trained in the particular skill will be required to perform the identified maintenance action.

n. Remarks---Additional information is provided to amplify the entries made in the form. Reference numbers pertain to the sources given in Section 4.0 of this document. A small letter entered in one of the other columns refers to a note in this column.

PRECEDING PAGE BLANK NOT FILMED.

SYSTEM: COMMUNICATIONS AND DATA MANAGEMENT		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MA AC	
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE
Unified S-Band Transponder	1		U					X	Loss of S-Band downlink & or up-link communic.	III	VHF backup. Earth re-entry vehicle comm. system.	X	X	X		X		X
S-Band Power Amplifiers (2 in 1 package)	1		U					X	Loss of power & degraded S-Band performance.	III	VHF backup.	X	X			X		X
S-Band Antenna	4	External						X	Loss of data or some experiments if multiple failures.	III	Multiple antennas.		X			X	No	
S-Band Receiver-Mixer	1		U					X	Decreased S-Band capability.	III	VHF backup.		X					
Up-Date Receiver-Decoder	1		U					X	Loss of ground up-date information to on-board computer & timer, & loss of ground commands.	II	Voice backup.	X	X			X		X
VHF Transponder (2 in 1 package)	4		U					X	Restriction of EVA. Loss of data & voice comm., & of comm. with EVA & logistics vehicle.	III	S-Band backup. Earth re-entry vehicle comm. system.	X	X			X		X
VHF Antenna	4	External						X	(See above)	III	None for EVA. S-Band to Earth.	X	X			X	No	
VHF Diplexer	1		U					X	(Same as VHF transponder)	III			X			X		
Rendezvous Radar Transponder	3		U					X	Reduce rendezvous capability.	III	Redundancy in L. Logistics vehicle system for backup.	X	X			X		X
Rendezvous Radar Antenna	3	External						X	(See above)	III	(See above)		X			X	No	
Audio Center	2 2	B	P					X	Reduced intercom	III	Use other center							X
Audio Center Control Unit	3 3	B	P					X	No comm. with that station.	IV	Other stations available.							X
Microphones and Headsets	3 3	B	P					X	Partial loss of comm. with that station	IV	Other stations available.							X

FOLDOUT FRAME # 1

DISPLAY	MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATIONS	MEDICAL	
		X		1.0						X	X	a					X		EOSS and JAG-I systems are essentially the same.
		X		1.0			X			X	X	a					X		a. Recommend modular design concept to reduce spares and replacement requirements. MTTR values are based on non-modular concepts. For modular concept, MTTR would be less.
	X	maintenance				X	b	X	X	c	c						X		b. It might be desirable to have an easy replacement concept for antennas in the event replacement proves a necessity.
				2.0													X		c. Safety and emergency procedures will be required for all EVA. See note (c) on Stability and Control System.
		X		1.0						X							X		
		X		1.0						X	X						X		
	X	maintenance				X	b	X	X	c	c						X		
																	X		
		X		1.0													X		
	X	maintenance				X	b	X	X								X		
		X		1.0													X		
		X		1.5													X		
		X		2.5													X		

SYSTEM: Communications and Data Management (Page 1 of 2)

FOLDOUT FRAME #2

SYSTEM: COMMUNICATION AND DATA MANAGEMENT (continued)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD			
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY
Premodulation Processor	1		U					X	Loss of part of all communication capability.	II	Internal backup modes for individual functions. Earth re-entry vehicle comm. system.	X	X	X		X
Central Timing Unit	1		U					X	Loss of time reference. Degraded performance of time-referenced equipment. Degraded a.c. power regulation.	II	Internal sync available at lower accuracy.		X			X
C-Band Transponder	1		U					X	Loss of continuous ground track capability.	III	"Skin tracking" capability by Earth C-Band equipment.		X			X
C-Band Antenna	1	External						X	(Same as above)	III		X				X
Signal Conditioning Unit	1		U					X	Loss of subsystem & experiment data.	II			X			X
Data Storage Units	3		U			X		X	Loss of some data storage capability	III						
Data Adapter	1		U					X	Degraded performance of spacecraft systems & experiments.	II	Built-in redundancy. Video communication. Ground station back-up.		X			X
Computer	1		U					X	(Same as above)	II	(Same as above)		X	X		
Hard Copy Printer and Computer Input Keyboard	1		U					X	Loss of manual input to computer.	III	Auto computer operation still available.		X			
PCM Telemetry Unit	1		U					X	Delay in data transmission to ground. Loss of data.	III	Data storage capability for transmission at later time.		X			X
TV Camera	2 2	B	 B					X		IV	Other cameras are portable.		X			
TV Monitor	[illegible]		U					X		IV	Multiple monitors.		X			
TV Pan and Tilt Mechanism	2 2	B	 B					X		IV						
Video Tape Recorder	1		U					X		IV						

FOLDOUT FRAME #2

ECTION HOD			MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATIONS	MEDICAL	
		X		X		1.0						X	X	a					X		
		X		X		1.0															
		X		X		1.5						X							X		
		X	X	Maintenance				X		X	X								X		
		X		X		1.0								a					X		
				X		1.0								a					X		
		X		X		1.0						X	X	a					X		Loss of data adapter or computer may restrict spacecraft operations to that which can be controlled manually. Special procedures may be required for periods when computer is inoperative. Modularization will result in minimum computer downtime.
				X		1.0						X	X	a					X		
			X	X	X	1.0					X			a					X		
		X				1.0								a					X		
						1.0													X		
						1.0													X		
						1.0									X						
						1.0								a					X		

SYSTEM: Communications and Data Management (Page 2 of 2)

FOLDOUT FRAME #2

SYSTEM: CREW SYSTEM		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAI ACT	
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE
Food Management																		
Storage Cabinets & Lockers		L						X	Seal leakage. Food contamination.	III	Multiple, independent cabinets.	X					X	
Oven		L						X	Excessive load-causing power shutdown.	III	Circuit breakers, fuses.		X					X
Refrigerator-Freezer		L						X	Food contamination.	II	Redundant power supply.		X					X
Bedding and Clothing		L						X	Flammability. Toxicity.	IV	Non-flammable materials.							X
Personal Hygiene																		
Storage Cabinets		L						X	Sharp corners. Toxic paint.	IV	Proper design.							X
Hygiene Enclosure		L						X	Loose water in cabin.	IV							X	
Enclosure Fan		L				X		X	Ineffective cleansing.	IV								X
Enclosure Filter		L						X	System contamination.	IV								X
Sponge Wetter and Rinser		L						X		IV								X
Personal Kit		L						X		IV							X	
Physical Conditioning		L						X		IV							X	
Recreation Equipment		L						X		IV							X	
EVA Equipment																		
Apollo Block II Suits	3 3 6	L	L					X	Loss of crew.	I	Present design incorporates safety provisions.	X	X	X			X	X
Apollo Block II PLSS	S	ame						X	Loss of crew.	I	(Same as above)	X	X	X				X
Umbilicals	12	L						X	Restriction in EVA operation.	II	PLSS has jettison capability.							X
Tethers, Restraints and Locomotion Aids	12	L						X	Increased effort for crew movement.	III								X
Crew Quarter Furnishings	4	L								IV							X	

FOLDOUT FRAME #1

GROUND DISPLAY	MAINTENANCE ACTION/TIME: REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	MAINT. CONSTR.: EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED	G.L. REQ'D.: SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	CREW SKILLS: MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATNS	MEDICAL	REMARKS
																			ECSS has a centrifuge and dry-wipe body cleaning.
																			CAS-1 has washable clothing and bedding, body washing, artificial-gravity station.
	X			1.0				d											1. Repair will require a special maintenance kit for structural items.
		X		1.5				X						X					If electrical wiring fails, its repair may be feasible.
		X		2.0										X					Failure may be due to loss of power supply, motor or compressor failure, or seal failure. Maintenance will be component replacement.
		X		0.5															
		X		0.5				d											
	X			0.5				d							X				
		X		1.0									X						Filter must be inspected and replaced periodically.
		X	X	1.5											X				Maintenance involves handling fluids.
		X		1.5			X		X						X				
	X			1.5															
	X			[illegible]									X						
	X			[illegible]									X						
	X	X		[illegible]				X	X	X	X				X				Maintenance could involve repair of fabric or replacement of soft components.
		X	X	[illegible]						X	X				X				Servicing of the PLSS O_2 supply, H_2O and LiOH will be required after each use. Total time available for each use is [illegible] hours.
		X		[illegible]						X	X				X				
		X		[illegible]									X						
	X			[illegible]				[illegible]					X						

SYSTEM: Crew System (Page [illegible] of [illegible])

FOLDOUT FRAME # 2

SYSTEM: ELECTRICAL POWER		MOD. LOC.			CRITICAL FAILURE MODE						
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS
Solar Panels	2	Interna						X	[illegible] solar panel power.	II	[illegible] Design [illegible] allowable [illegible] radiation [illegible] space environment.
Batteries, Ni-Cad	3		L					X	Loss of battery power. H_2 gas & KOH gas. Overpressure & rupture. Fire, smoke.	I	Auto isolation. Reduce power [illegible] Fire detection [illegible] Battery venting. Battery [illegible]. Voltage & [illegible] monitors.
Inverters (Solid-State)	3		L					X	Loss of a.c. power.	III	Failure [illegible] Reduce power [illegible] Disconnect [illegible]
Voltage Regulator, Shunt	2		L					X	Loss of regulated d.c.	II	
Failure Sensors, VR	2		L		X	X			Loss of regulated d.c.	II	
Main Contactors	8		L			X		X	Loss of some or all power. Fire, smoke.	II	Voltage & current [illegible] Auto [illegible] critical [illegible]
Battery Charger (BC)	3		L					X	Loss of [illegible] power.	III	Failure [illegible] Disconnect [illegible] circuit.
BC Contactor	3		L			X			Loss of some battery power.	III	Auto [illegible]
BC Failure Sensor	3		L		X	X			Loss of some battery power.	III	
BC Reverse Current Relay	3		L					X	Discharge battery [illegible].	III	
Power Inverter	1		L			X		X	[illegible]	III	

FOLDOUT FRAME #1

DETECTION METHOD			MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATIONS	MEDICAL	
X			No maintenance									e		X		X					EOSS and JAC-I electrical power systems are the same. d. Solar panels will present a physical hazard to EVA and docking operations. f. Special procedures will be required for maintenance on electrical power system components to preclude possible injury to crew or loss of all power. Special procedures also required if smoke or fire involved; shut off fans, use fire extinguisher, pressure suits, depressurize cabin, etc. (Ref. 111). g. From a safety standpoint, it may be desirable to locate components which could cause a fire in unpressurized areas of the spacecraft, even though this might complicate accessibility for maintenance.
X				X	X	2.5			X	X	f	X	X	g	X	X					Batteries have one year life and must be replaced at this interval. Would be advantageous to have capability to replace individual battery cells for random failures (Ref. 46).
				X		1.3					f					X					
				X		1.5					f					X					Individual phases of the inverters will be spared, so replacement of an entire inverter will not be required (Ref. 47).
				X		1.0					f					X					
X			Redundancy only						X			X	X	g							
				X		1.0					f					X					
			Redundancy only																		
				X		1.0										X					
				X		1.5										X					
				X		1.0					f					X					

SYSTEM: Electrical Power (Page 1 of 2)

FOLDOUT FRAME #2

SYSTEM: ELECTRICAL POWER (continued)		MOD. LOC.			CRITICAL FAILURE MODE								
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	DETEC METH ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE
Buses, Fuses, Circuit Breakers			L			X	X		Short circuit, overload. Fire, smoke. Loss of power.	I	Auto. disconnect. Non-flammable materials. Fire detection system. Manually isolate bus. Voltage & current monitors.		X	X
Wiring and Connectors								X	(Same as above)	I	Non-flammable materials. Fire detection system. Fuses, CB's. Current limiters.	X		X
Rotational Mechanism and Support Arms		External						X	Loss of some or all solar panel power.	II	CMG or RCS can orient spacecraft to point panels at sun.	X	X	X

FOLDOUT FRAME #1

REDUNDANCY RECOM.	DETECTION METHOD				MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWN TIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATNS	MEDICAL	
	X	X	X			X		[illegible]					f	X	X	g		X					—
X		X	X			X		3.0			X		f	X	X			X					
X	X	X			X	X		[illegible]		X	X		h	X	X		X	X					h Maintenance may involve replacement of electric motor, or repair of damage to support arms which will require special tools.

SYSTEM: Electrical Power (Page 2 of 2)

FOLDOUT FRAME #2

SYSTEM: ENVIRONMENTAL CONTROL/LIFE SUPPORT SYSTEM (EC/LSS)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD			
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND
CO_2 Removal																
Silica Gel Canister	4		L					X	Fluid leakage. Contamination of mol sieve beds. CO_2 increase.	III	High R. Multiple canisters.					
Mol Sieve Canister	4		L					X	Zeolite leakage. Atmosphere contamination. CO_2 increase.	III	High R. Multiple canisters.		X			
Gas Valves	8		L			X	X		O_2 leakage. Reduce CO_2 removal capacity.	III	Multiple canisters.		X			
Timer and Valve Control	2		L					X	CO_2 increase.	II		X	X			
Valve Assembly, Coolant	4		L			X	X		CO_2 increase. Fluid leakage.	II		X	X			
Mol Sieve Isolation Valve	2		L				X		Cabin air leakage. CO_2 leakage.	II	Manual control.	X	X			
Vacuum Pump	1		L			X			Loss of cabin air.	II			X			
Plumbing	1		L					X	Fluid leakage.	II	Redundancy for critical circuits. Isolation capability.					
Atmosphere Purification and Suit Loop																
Suit Circuit Return Valve	2		L					X	Leakage of O_2 in depressurized cabin condition.	III	Built-in redundancy			X		
Debris Trap	2		L					X	Contamination of downstream components.	III	PLSS					
Cabin Return Valve	4		L			X			Cannot use suit loop.	II	Manual operation. PLSS.		X			
Suit Compressor	4		L			X		X	Loss of air flow to suits.	II	PLSS. Air flow monitor.	X	X	X		

FOLDOUT FRAME #1

DETECTION METHOD			MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D			CREW SKILLS						REMARKS
VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC.	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATIONS	MEDICAL	
																					The EC/LSS for EOSS is basically the same except that it has 2 redundant systems and only humidity water is processed. The JAG-I EC/LSS uses a 20/80-O_2/N_2 14.7-psia atmosphere, equipment in atmosphere cooled and all water is reclaimed with separate processing. The SLSS baseline system shown here consists of 2 three-man systems with all items located in the same compartment. If one system fails, the other could supply the 3-man requirements for a limited period of time (2-3 days). For safety considerations, it would be advisable to locate the two EC/LSS in separate compartments which can be isolated from each other.
				X		3.0			X								X				Requires breaking hot and cold water lines
				X	X	2.0			X								X				Zeolite may require replacement periodically. Replacement involves containment of zeolite material.
				X		1.5			X								X				Requires breaking O_2 line.
				X		0.5						X					X				
				X		2.0			X			X		i			X				Requires breaking hot and cold water lines
				X		3.0		X			X	X					X				Requires breaking line exposed to vacuum. Therefore, should only replace if redundant valve also fails; or when cabin is depressurized for some reason.
				X		1.5			X						X						
			X			2.0			X	X	X	X		i	X		X				i. The silica gel canisters, coolant valve assemblies and the plumbing between these will be alternately subjected to temperatures as low as 40-50°F or as high as 300-400°F. These items must be designed with this environment in consideration.
X				X	X	0.5			X			X	j				X				
				X	X	1.0			X		X		j	X			X				j. These items are usually used only in emergencies; i.e., when it is necessary to use the suit loop because of contaminated cabin air. The suit loop should be checked periodically to verify operation. The debris trap will require cleaning and/or replacement at intervals dependent on use of the suit loop.
				X		1.0			X				j	X							
X				X		2.0			X				j								

SYSTEM: Environmental Control/Life Support (Page 2 of 4)

FOLDOUT FRAME #2

SYSTEM: EC/LSS (continued)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAIN ACTIO	
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE
Atmosphere Purification and Suit Loop (continued)																		
CO_2 Absorber Element	12		L					X	Increased CO_2 concentration.	III	CO_2 monitor. Replaceable element. PLSS.	X	X	X				X
CO_2 Absorber Canister	2		L					X		III	High R.	X						X
Suit Bypass Valve	2		L			X			Incorrect suit flow.	III	PLSS. Individual suit controls. Repressurize cabin.							X
Suit Isolation Valve, Sol.	2		L		X	X			Cannot isolate crew member from suit circuit or inadvertent isolation.	IV	PLSS. Manual operation.							X
Atmosphere Purification Fan	2		L					X	Loss of air flow. Contamination build-up.	II	Suit loop. PLSS. Airflow monitor.	X						X
Orifice	2		L			X			Reduced air flow.	III	High R.						No	ma
Debris Trap and Charcoal Filter	2		L					X	Contamination of downstream items. Reduced air flow.	III	Replace filter. Orifice allows some flow.							X
Suit HX Assembly	2		L					X	Increased humidity. Water leakage. Increased temp. of suit loop air flow.	II	Humidity monitor. High R.	X						X
Flow Limiter	6		B					X	Incorrect suit flow.	III	Flow monitor. High R. Multiple locations each compartment.		X				No	ma
Suit Hose Connectors	6		B					X	O_2 leakage. Usable for suit.	III	Flow monitor. High R. Multiple location each compartment.		X					X
Catalytic Burner	2		L					X	Increase in trace gases.	II	Continuous monitor of gas levels. Suit loop. PLSS.		X	X				X

FOLDOUT FRAME #1

MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC.	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATNS	MEDICAL	
	X	X	0.2			X		X		J				X				Each element good for approximately 12 hours. Quantity of 12 sufficient for 3 days emergency operation.
	X		2.0			X				J				X				
	X		1.0			X				J				X				
	X		1.5							J				X				
	X		2.0			X			X					X				Design to permit replacement of one fan while other is operating.
No maintenance						X	X							X				Orifice welded in. Very remote chance of failure.
	X	X	0.2			X	X	X			X			X				Filter will require replacement at regular intervals. Should be able to replace with system operating. Tools and procedures must provide for debris control.
	X		4.0			X	X	X	X	X	X							Replacement requires breaking water lines and O_2 lines.
No maintenance												X						Flow limiter welded in. Very remote chance of failure.
	X		1.0			X	X							X				Only 6 indicated for SV-SLSS, although 12 space suits (located 3 in each of 4 compartments) were provided. Three suit connectors should also be provided in each of the 4 compartments.
	X	X	2.0 1.0					X	X	X	X			X				Depending on failure, it may be necessary to allow burner to cool off (10-15 hours) before maintenance. If contamination gets too high, crew may have to go on suit loop or PLSS. Burner catalyst must be replaced at regular intervals (approximately 60 days).

SYSTEM: Environmental Control/Life Support (Page 2 of 4)

FOLDOUT FRAME #2

SYSTEM: EC/LSS (continued)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAIN ACTIO	
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE
Atmosphere Purification and Suit Loop (continued)																		
Cyclic Accum. Valve Assy.	4		L					X	O_2 leakage. Humidity increase.	III	Manual control.		X					X
Cyclic Accum. Valve Control	4		L					X	Humidity increase.	III	Manual valve operation.							X
O_2 Warning Sensor	2		L					X	Undetected O_2 leak.	II	O_2 monitor.	X	X	X				X
O_2 Sensor Signal Cond.	2		L					X	No O_2 leak warning.	II	Check other indicator.	X	X	X				X
Plumbing	1	B	B					X	Leakage.	II	Redundancy for critical circuits. Isolation capability.						X	
Cabin Heat Transport Loop																		
Water Check Valve	6		L				X		Reduces temp. control capability of cabin HX.	III	Only ½ of capability affected. Isolate failed loop.	X	X	X				X
Temperature Control Valve	4		L					X	Loss of cabin temperature control.	III	(Same as above)	X	X	X				X
Water Temperature Sensor	2		L					X	Freezing water in transport loop.	III	Temperature monitored more than one place.	X	X	X				X
Water Fill Connection	4		L					X	Water leakage.	III	Only used to fill tanks.	X						X
Water Shutoff Valve	8		L					X	Cannot isolate reservoir or cannot use contents. Leakage. Cannot refill tanks.	III	Water stored in more than one tank.							X
Water Reservoir	2		L					X	Loss of water supply. Diaphragm rupture: O_2 in water lines H_2O in O_2 lines.	II	Quantity monitor. Shutoff valves. Check valves. Water stored in more than one tank.	X	X	X			X	
Evaporator Back Pressure	2		L					X	Inefficient evaporation operation. Excessive water use. Cabin air leakage.	III	Two evaporators are in system.	X	X	X				X
Back Pressure Control	2		L					X	Excessive water use. Water temperature not kept in limits.	III	Two evaporators are in system.	X	X	X				X

FOLDOUT FRAME #1

	MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED	SAFETY PROCED	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATNS	MEDICAL	
		X		1.0			X		X						X				Replacement involves breaking O_2 lines.
		X		0.5											X				
		X		0.5											X				
		X		0.5											X				
	X			2.0			X	X	X				X		X				Procedures and special repair kits must be developed for repairing leaks in O_2, H_2 and water (hot and cold) lines in a 0-g environment.
		X		1.0			X		X						X				X. Requires breaking water lines.
		X		2.0			X		X						X				
		X		1.5			X	X	X						X				Tubing repair tools and procedures will be needed if tubing rupture occurs from freezing.
		X		2.5		X	X	X	X	X			X		X				Used only at resupply.
		X		1.5					X						X				
	X			2.0				X	X	X	X	X			X				Need to contain water while replacing diaphragm. May require purging of O_2 or H_2O lines. If all tank diaphragms ruptured, mission abort may be required.
		X		2.5		X	X	X	X	X			X		X				One end of valve is vented to space. Therefore, replacements will require depressurization of cabin unless installation can be designed to avoid it.
		X		1.0											X				

SYSTEM: Environmental Control/Life Support (Page 3 of 4)

FOLDOUT FRAME #2

SYSTEM: EC/LSS (continued)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAIN ACTIO	
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE
Cabin Heat Transport Loop (continued)																		
Wick Temperature Sensor	2		L					X	Excessive water use. Water temperature not kept in limits.	III	Built-in redundancy.		X					X
Water Temperature Sensor	4		L					X	Water temperature not kept in limits.	III		X	X	X				X

FOLDOUT FRAME # 1

REDUNDANCY RECOM.	DETECTION METHOD				MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.I. REQ'D.			CREW SKILLS						REMARKS
	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED	SAFETY PROCED	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICATIONS	MEDICAL	
	X					X		1.0					X						X				
X	X	X				X		1.0					X						X				

SYSTEM: Environmental Control/Life Support (Page 4 of 4)

FOLDOUT FRAME #2

SYSTEM: STABILITY AND CONTROL SYSTEM		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAINT ACTION		
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE
Sensors																			
Body-Mounted Attitude Gyro (BMAG) Package	1		U					X	Instability.	III	Manual control.		X					X	
BMAG Electronics	1		U					X	Instability.	III	Manual control.		X					X	
Horizon Scanner	1			X				X	Instability.	III	Manual control.	X	X	X				X	
Horizon Scanner Electronics	1		U					X	Instability.	III	Manual control.	X	X					X	
Controls and Displays																			
Attitude Indicator	1		U					X	Display errors.	III			X					X	
System Status	1		U					X	Display errors.	III			X					X	
ΔV Set	1		U			X				III	Manual control.		X					X	
Manual Attitude Controller	1		U			X	X	X	Tumbling.	II	Limit control. Cutoff switch. Auto. control.		X	X		X		X	
Attitude Set Control	1		U			X				III	Manual control.		X					X	
Display Electronics Assembly	1		U					X	Display errors.	III			X					X	
Control-Moment Gyro (CMG)																			
CMG	3			X				X	Instability. Loss of solar panel orientation.	II	Only 2 required for control. RCS is alternate. Isolate affected CMG		X					X	
CMG Power Inverter	2		U					X	Loss of CMG.	II	(Same as above)		X					X	
CMG Gimbal Servo Electronics	[illegible]		U					X	Partial loss of CMG.	II	(Same as above)		X					X	

FOLDOUT FRAME #1

MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWN-TIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICAT'NS	MEDICAL	
																			EOSS and JAC-I Differences Both use Earth-storable hypergolic propellants, N_2O_4 and MMH. These propellants will impose additional hazards over a cold gas (N_2) system, e.g., fire, fluid contamination during maintenance (Ref. 55). The major hazard of the cold gas system is the high pressure level required.
		X		1.0			X		X							X			
		X		0.5															
		X		3.0		X	X	m	m	o						X			m. May require special alignment to replace. Recommend redundancy only, no spares (Ref. 65).
		X		0.5												X			
		X		1.0												X			
		X		0.7												X			
		X		1.0												X			
		X		1.5			X				X			X					No manned control until replaced.
		X		1.0												X			
		X		0.5												X			
		n		4.0		X	X		n	o		n	X			X			n. Size of CMG precludes movement of spares for replacement. Spares should be placed in operable location and pre-wired so that activation requires only orienting in proper axis and switching CMG into system. CMG too heavy to provide multiple redundancy for each. Most effective maintenance of CMG would be capability to replace critical components instead of whole CMG as discussed in Ref. 48.
		X		0.7										X					
		X		0.5												X			
																			o. Special procedures will be required for all EVA; aids to maneuver around obstructions, restriction on firing of thrusters, limitations during solar activity periods, lighting requirements, visual monitoring of EVA, orientation for radiation protection.

SYSTEM: Stability and Control (Page 1 of 2)

FOLDOUT FRAME # 2

SYSTEM: STABILITY AND CONTROL SYSTEM (continued)		MOD. LOC.			CRITICAL FAILURE MODE								DETECTION METHOD				MAINT ACTIO		
NOMENCLATURE	QUANTITY	LABORATORY	CORE	AFT BAY	PREMATURE OPERATION	FAILURE TO START OPERATING	FAILURE TO STOP OPERATING	FAILURE DURING OPERATION	POTENTIAL HAZARD/ EFFECT	HAZARD CATEGORY	SAFETY PROVISIONS	REDUNDANCY RECOM.	ONBOARD DISPLAY	VISUAL/AUDIBLE WARNING DEVICE	AUTO. ABORT SENSING DEVICE	GROUND DISPLAY	REPAIR	REPLACE	SERVICE
Reaction Control System (RCS)																			
Thruster Assembly (incl. 3 thrusters)	4			X		X	X		Tumbling. Crew sickness. Excessive docking loads. Loss of solar panel orientation. Loss of experiment data.	II	Temperature monitor. Auto. cutoff. Isolate failed jet.	X	X	X	X	X		X	
Regulators, Pressure	4			X				X	Partial loss of RCS.	II	Isolate from pressure when not in use. Pressure monitor.	X	X					X	
Solenoid	4			X		X	X		Partial loss of RCS.	II		X	X					X	
Shutoff Valves	4			X		X			Partial loss of RCS.	II		X	X					X	
Valves, Relief	4			X		X	X		Partial loss of RCS.	II		X	X					X	
Driver Electronics	1			X		X	X		Inoperative RCS. Tumbling.	II	Auto. cutoff.	X	X	X				X	
Propellant Storage and Distribution																			
Filters	4			X				X	Flow restriction. Erratic thruster operation.	III		X	X					X	
Tubing and Plumbing	1			X				X	Propellant leakage. Fire.	II	Shutoff valves.	X	X	X			X		
Tanks (High Pressure) With Propellant	8			X				X	Meteoroid penetration. Explosion, fire. Propellant leakage. Tumbling.	I	Pressure monitor. Shielding. Tank separation. Fire detection system.	X		X	X	X	[illegible]	[illegible]	

FOLDOUT FRAME #1

	MAINTENANCE ACTION/TIME					MAINT. CONSTR.				G.L. REQ'D.			CREW SKILLS						REMARKS
GROUND DISPLAY	REPAIR	REPLACE	SERVICE	MTTR (HOURS)	MAXIMUM DOWNTIME	EVA/PRESSURE SUIT	ACCESSIBILITY	SPECIAL TOOLS	SPECIAL PROCED.	SAFETY PROCED.	EMERGENCY PROC	SAFETY DESIGN	MECH./STRUCT.	ELECTRICAL	EC/LSS	GUID. & NAVIG.	COMMUNICAT'NS	MEDICAL	
																			Use of cold nitrogen gas for RCS reduces the hazard involved in replacing components. However, because of necessity for EVA, it is recommended that at least one level of redundancy be provided to reduce need for EVA.
																			MTTR estimates assume that RCS components are designed for replacement.
X		X		4.0		X	X		X	o			X			X			Maintenance must consider the possible hazard involved with cold nitrogen gas. Thruster location design must consider the exhaust plume effects on spacecraft equipment, (e.g., solar arrays, antennas).
		X		3.0		X	X		X				X			X			
		X		3.0		X	X		X	o			X			X			
		X		3.0		X	X		X	o			X			X			
		X		3.0		X	X		X	o			X			X			Rather than have valves to enable isolation of each RCS component, probably could have one valve at upstream end of system which would cut off gas flow to all downstream components.
		X		4.0		X	X		X	o			X			X			
		X		3.0		X	X		X	o			X			X			
	X			4.0		X	X	X	X	o			X						Special repair kits will be used instead of spares. May involve use of adhesive or welded patches, or use of cutting tool and replacement of tubing section.
X	No maintenance																		May be able to provide resupply capability for propellants.
																			Desire to have tank separation so that explosion of one tank will not endanger others.

SYSTEM: Stability and Control (Page 2 of 2)

FOLDOUT FRAME #2

APPENDIX B

APPLICABLE LOGIC DIAGRAM AND FAULT TREE STATEMENTS

As a convenience for reviewing the safeguards given in Chapter 3.3 of this document, certain statements from the Logic Analysis, D2-113070-9, and the Fault Tree Analysis, D2-113070-10, are repeated in this appendix to reduce the need for having those two volumes at hand. However, if it is desired to gain more than a cursory acquaintanceship with the relationships between these analyses, it is recommended that the referenced documents be used to determine the actual contexts and semantic environments of the statements given here.

1.0 STATEMENTS EXTRACTED FROM LOGIC DIAGRAM, D2-113070-9

Proposition No.	Proposition Statement
4C	Crew members will be able to perform all crew tasks necessary to sustain life.
4D	Normal ground systems will be capable of performing all ground support functions necessary to crew survival. (T2)
6B	Special remedial systems will protect all crew members from all potentially fatal immediate danger not prevented by normal systems.
8C	Special remedial systems will protect all crew members from all directly fatal decompression not prevented by normal systems.
8D	Special remedial systems will protect all crew members from all directly fatal heat exposure not prevented by normal systems.
8E	Special remedial systems will protect all crew members from all directly fatal radiation exposure not prevented by normal systems.
8F	Special remedial systems will protect all crew members from all directly fatal overpressure not prevented by normal systems.
8H	Special remedial systems will protect all crew members from all directly fatal exposure to chemicals not prevented by normal systems.

Proposition No.	Proposition Statement
9B	All spacecraft subsystems will perform their respective spaceflight operational functions in the manner necessary to ensure crew survival.
9C	All hardware interfaces among internal equipment will perform their respective spaceflight operational functions in the manner necessary to ensure crew survival.
9D	All hardware interfaces among external equipment, and other orbital space vehicles, will perform their respective spaceflight operational functions in the manner necessary to ensure crew survival.
9E	All man/machine operational interfaces will perform their respective spaceflight functions in the manner necessary to ensure crew survival.
9F	All scheduled and unscheduled maintenance functions pertaining to the orbital space system will be performed in the manner necessary to ensure crew survival.
9G	All on-board support resources required during spaceflight operations will perform in the manner necessary to ensure crew survival.
10D	All spacecraft subsystems will be designed and produced to conform with operational parameters which will ensure crew survival.
10F	Any spacecraft subsystem which requires built-in redundancy to perform within acceptable tolerances continuously throughout the orbital mission will have the necessary redundancy incorporated.
10G	Any spacecraft subsystem which requires inflight maintenance to perform within acceptable tolerances continuously throughout the orbital mission will be maintainable in the operational environment.
11B	Special remedial systems will protect all crew members from any immediate danger of directly fatal collision.
11E	Special remedial systems will protect all crew members from any immediate danger of directly fatal physiological stress due to tumbling, rotation, or linear motion.

Proposition No.	Proposition Statement
12E	Special remedial systems will perform all corrective actions necessary to sustain life that are not performed by assigned crew members.
13C	Special remedial systems will protect all crew members from any immediate danger of directly fatal collision of spacecraft equipment with crew members.
13D	Special remedial systems will protect all crew members from any immediate danger of directly fatal collision of flying debris with crew members.
13F	Special remedial systems will protect all crew members from any immediate danger of directly fatal collision between one crew member and another.
14B	No immediate danger of crew loss will exist.
15C	There will be no immediate danger of direct crew loss from lack of vital supplies.
15E	There will be no immediate danger of direct crew loss from lack of oxygen.
15K	There will be no immediate danger of the rate of supply of breathable oxygen to any crew member decreasing below the rate necessary to sustain life.
16C	There will be no immediate danger of directly fatal exposure of any crew member to decompression.
16D	There will be no immediate danger of directly fatal exposure of any crew member to heat.
16F	There will be no immediate danger of directly fatal exposure of any crew member to overpressure. (T4.1)
16H	There will be no immediate danger of directly fatal exposure of any crew member to chemicals.
17E	There will be no immediate danger of directly fatal physiological stress from tumbling, rotation, or linear motion.
18D	There will be sufficient time for available crew members to accomplish any human task necessary to sustain life.

Proposition No.	Proposition Statement
18E	All necessary resources will be available to any crew member performing any human task necessary to sustain life.
21B	No crew member will contract any potentially fatal infection during his orbital stay.
21D	No crew member will contract any infectious illness during his orbital stay.
22D	There will be adequate medical facilities in the spacecraft to treat any potentially fatal illness contracted by any crew member during his orbital stay.
23D	There will be adequate medical facilities in the spacecraft to treat any potentially fatal injury sustained by any crew member during his orbital stay.
24I	No crew member will be injured by overpressure. (T4.1)
27C	The crew members available to perform tasks necessary to sustain life will not have been incapacitated by direct physical impairment from external causes.
27E	No human task necessary to sustain life will be beyond the physical capability of normal people.
28C	The locations and activities of crew members will make technically capable crew members available for performing any human task necessary to sustain life.
28G	There will be at least one crew member technically capable of performing any extra-vehicular human task necessary to sustain life.
30C	The temperature environment of each crew member will permit vital basic metabolism and thermal control functions of a normal untrained human body.
30D	Edible food and potable water will be accessible to all crew members under conditions that permit eating and drinking by normal untrained people sufficiently to sustain life.
30E	The environment of any crew member will not prevent sufficient elimination of body wastes to sustain life by any normal untrained person.

Proposition No.	Proposition Statement
31G	No crew member will become physically ill during his orbital stay due to infection.
32B	No crew member will be injured by exposure to chemicals during his orbital stay.
32C	No crew member will be injured by any form of relative motion during his orbital stay.
32D	No crew member will be injured by heat during his orbital stay.
32E	No crew member will be injured by radiation during his orbital stay.
33E	Any immediate danger of any crew member being subjected to directly fatal lack of oxygen will be potentially correctable.
33I	Special remedial systems will be potentially capable of supplying any immediate oxygen needs of any crew member not supplied by normal systems.
34C	Any immediate danger of any crew member being subjected to any directly fatal decompression will be potentially correctable.
34I	Any immediate danger of any crew member being subjected to directly fatal exposure to chemicals will be potentially correctable.
35B	Any immediate danger of directly fatal collision will be potentially correctable.
35E	Any immediate danger of directly fatal physiological stress from tumbling, rotation, or linear motion will be potentially correctable.
38C	There will be no potentially dangerous sources of radiation on-board the spacecraft other than nuclear power plants for the generation of spacecraft power. (T4.1)
40B	A solar radiation warning system will not fail to provide signals, recognizable by each crew member as instruction to seek protection, in time for all crew members to go to a shielded haven in the spacecraft before solar radiation becomes of fatal type and intensity.

Proposition No.	Proposition Statement
40C	There will be one or more havens in the spacecraft that are shielded from all potentially fatal solar radiation and capable of holding all crew members.
42D	Special remedial systems will supply to all crew members all immediately necessary oxygen not supplied by normal systems.
42H	Normal systems will maintain immediately necessary oxygen by replacing oxygen that is consumed, dissipated, or removed from the volume immediately available to each crew member.
43F	There will be no failure of normal systems for storing and conducting to crew members replacement oxygen for any immediately necessary oxygen that is consumed, dissipated, or removed from the volume immediately available to each crew member and not replaced from oxygen salvaged from atmospheric gas removed from crew locations.
44B	Atmospheric gas whose contaminant level permits breathing without physical illness by normal untrained people will be supplied to each crew member.
44C	Atmospheric gas whose partial pressure of oxygen permits breathing without physical illness by normal untrained people will be supplied to each crew member.
44D	Atmospheric gas whose temperature permits breathing without physical illness by normal untrained people will be supplied to each crew member.
44E	Atmospheric gas whose total pressure permits breathing without physical illness by normal untrained people will be supplied to each crew member.
45B	Any atmospheric gas, in crew locations that are being contaminated with any material that prevents its safe breathing, will be removed or diluted at a rate that enables continued breathing by normal untrained people without illness.
45E	All crew members will be removed, rapidly enough to prevent illness, from any location whose atmosphere is becoming contaminated with any material that prevents safe breathing by normal untrained people.
46B	Any equipment features whose manipulation is an extravehicular human task necessary to sustain life will be accessible and operable by a normal person.

Proposition No.	Proposition Statement
46D	Any equipment features whose manipulation is an intra-vehicular human task necessary to sustain life will be accessible and operable by a normal person.
47E	Any equipment in the spacecraft whose manipulation is a non-routine task necessary to protect crew members from directly fatal physical injury from external causes will be accessible and operable by normal people.
48B	The spacecraft structure will permit access by a normal person to any equipment in the spacecraft whose manipulation is necessary to provide vital supplies to any crew member.
48C	Arrangement of equipment in the spacecraft will permit access by a normal person to any equipment in the spacecraft whose manipulation is necessary to provide vital supplies to any crew member.
48E	Any equipment item, materials, supplies, spare parts or tools whose manual transportation is necessary to provide vital supplies to any crew member will be transportable by normal people.
48F	Any opening, closing, removal, replacement, disassembly, or assembly operation in the spacecraft necessary to provide vital supplies to any crew member will be performable by normal people.
48H	Any visual indicators on equipment in the spacecraft whose recognition is essential to properly perform operations necessary to provide vital supplies to any crew member will be clearly visible to persons with normal sight.
48I	Any auditory signals from equipment in the spacecraft whose recognition is essential to properly perform operations necessary to provide vital supplies to any crew member will be clearly audible to persons with normal hearing.
50E	All vital crew tasks not performed by assigned crew members using designated equipment will be performed by other means.
51B	Systems produced and used for some other basic purpose will protect all crew members, not protected by normal or special remedial systems, from all immediate danger of directly fatal injury from external causes.
52B	There will be no immediate danger of directly fatal collision of meteoroids with crew members.

Proposition No.	Proposition Statement
52C	There will be no immediate danger of directly fatal collision of spacecraft equipment with crew members.
52D	There will be no immediate danger of directly fatal collision of flying debris with crew members.
53E	There will be no immediate danger of directly fatal collision of the spacecraft proper with crew members due to spacecraft rotation.
57B	Shielding of nuclear power plants on the spacecraft will be sufficient to prevent any nuclear excursion from constituting an immediate danger of directly fatal radiation exposure of any crew member.
57D	Containment vessels will not permit fluid radioactive materials to leak from shielded spacecraft nuclear power reactor compartments into crew areas.
57E	The effectiveness of spacecraft nuclear power reactor shielding in preventing fatal crew member exposure will not be destroyed by structural damage.
57F	No crew member will be in immediate danger of directly fatal radiation exposure during repair, refurbishment, or refueling of spacecraft nuclear power reactors.
58D	Nuclear excursions of spacecraft primary power reactors will never exceed the upper limit of power excursion levels specified to activate all emergency backup controls.
59B	There will be no immediate danger of any crew member swallowing any poisonous chemical that would be directly fatal.
59D	There will be no immediate danger of the skin surface of any crew member being contaminated with any chemical that would be directly fatal.
59F	No crew member will be in immediate danger of directly fatal exposure of large areas of his body to any poisonous or corrosive chemical.
60D	Any supplies, materials for experiments, or spacecraft materials that constitute a deadly contact poison will be kept contained and controlled in a manner that does not present any immediate danger to the life of any crew member.

Proposition No.	Proposition Statement
60E	Any deadly contact poison that is generated by accident or by any experimental, housekeeping, spacecraft operation, or logistics activity will be contained and controlled in a manner that does not present any immediate danger to the life of any crew member.
61B	No supplies, materials for experiments, or spacecraft materials will constitute a poison that would be directly fatal if breathed.
61D	Any supplies, materials for experiments, or spacecraft materials that constitute a poison that would be directly fatal if breathed will be contained or controlled in a manner that does not present any immediate danger to the life of any crew member.
61E	Any poison generated by accident or by any experimental, housekeeping, spacecraft operation, or logistics activity that would be directly fatal if breathed will be contained or controlled in a manner that does not present any immediate danger to the life of any crew member.
65D	Any immediate danger of directly fatal collision of flying debris with crew members will be potentially correctable.
69J	Crew members will perform all medical tasks necessary to treat critical injuries. (T4.1)
70J	Crew members will perform all medical tasks necessary to treat critical infections. (T4.1)
76C	No crew member will be incapacitated by exposure to chemicals.
76J	No crew member will be incapacitated by exposure to any toxic chemical.
76K	No crew member will be incapacitated by exposure to any noxious chemical.
78G	No crew member will suffer disabling impairment of vision due to exposure to light.
80B	Special remedial systems will provide means of travel, or escape, to a safe haven in the spacecraft in case routine means are inadequate.

2.0 UNDESIRED EVENTS EXTRACTED FROM FAULT TREE, D2-113070-10

Event No.	Event Statement
1.1-C	Crew members are exposed to decompression.
1.1-D	Decompression eventuates from loss of spacecraft pressure supply.
1.1-E	Decompression results from failure of spacecraft pressure retention.
1.1-F	Decompression eventuates from failure of pressure suit supply.
1.1-G	Decompression results from failure of pressure suit pressure retention.
1.1-J	Failure of pressure retention results from failure of structural matrix.
1.1-L	Crew exposed and protective action not accomplished through use of emergency equipment.
1.1-M	Crew exposed and protective action not accomplished through emergency procedures.
1.2-B	Loss of pressure suit pressure retention results from suit assembly failure.
1.2-C	Loss of pressure suit pressure retention results from suit damage.
1.2-G	Damage results from pressure suit tear.
1.3-C	Structural matrix failure results from damage during space operations.
1.3-G	Failure results from meteoroid impact.
1.4-C	Failure results from loss of subsystem function.
1.4-F	Loss of subsystem function results in spacecraft pressure dump.
1.5-C	Emergency equipment is nonexistent at time required.
1.5-E	Emergency equipment inoperative due to damage from effects of decompression.
1.7-G	Damage results from logistic support operations.
1.7-K	Damage occurs during logistic vehicle docking operations.

Event No.	Event Statement
1.12-D	Explosive failure of liquid system results from inadequacy of system location.
2.1-B	Crew members are injured thru exposure to potentially fatal heat.
2.3-D	Injury results from exposure to heat generated by chemical reaction.
2.3-J	Injury results from fire occurring within a normally manned area of spacecraft.
2.5-D	Electrical System component heated through electrical system fault.
2.6-D	Fire occurs of a hypergolic or pyrophoric nature.
2.6-F	Fuel, oxygen, and ignition source are provided as separate entities.
2.6-G	Combustible materials are present (fuel source).
2.7-B	Injury results from failure to control fire.
2.7-I	Escape action is not facilitated by fire emergency procedures.
2.7-H	Explosive combination of materials and environment exists.
2.8-G	Equipment is inoperative due to damage effects of fire.
2.8-H	Equipment is not automatically activated.
2.9-P	Emergency fire control action is not facilitated by the fire emergency warning system.
2.10-D	The fire warning system is inadequate at the time required.
2.11-E	An electric power source produces an electrical arc for ignition.
2.15-G	Operational breakdown results from high temperature exceeding functional capability of subsystem.
2.17-C	Fire results in overtaxing equipment operation.
3.1-M	Crew members lack radiation protection due to inadequate radiation shielding.

Event No.	Event Statement
3.2-H	Flare-produced high energy solar particles are present.
3.3-J	A nuclear induced artificial orbital radiation environment is present.
3.4-D	Deficient personnel radiation exposure monitoring provisions (dosimetry).
3.4-G	Accumulated radiation exposure not recognized.
3.5-C	Crew members lack radiation shielding while exterior to the spacecraft.
3.5-H	Shielding is not adequate, by design, to protect against the expected environment.