

NASA Contractor Report 3858

NASA-CR-3858 19850019618

Space Station Crew Safety Alternatives Study—Final Report

Volume V—Space Station Safety Plan

G. H. Mead, R. L. Peercy, Jr.,
and R. F. Raasch

CONTRACT NAS1-17242
JUNE 1985

LIBRARY COPY

JUN 11 1985
LANGLEY RESEARCH CENTER
LIBRARY, NASA
HAMPTON, VIRGINIA

NASA

NASA Contractor Report 3858

Space Station Crew Safety
Alternatives Study—Final Report

Volume V—Space Station Safety Plan

G. H. Mead, R. L. Percy, Jr.,
and R. F. Raasch

*Rockwell International
Downey, California*

Prepared for
Langley Research Center
under Contract NAS1-17242



National Aeronautics
and Space Administration

Scientific and Technical
Information Branch

1985

FOREWORD

This report is one of five documents covering the results of the Space Station Crew Safety Alternatives Study conducted under Contract NAS1-17242. The study documentation is designated as follows:

- Vol. I - Final Summary Report (NASA CR-3854)
- Vol. II - Threat Development (NASA CR-3855)
- Vol. III - Safety Impact of Human Factors (NASA CR-3856)
- Vol. IV - Appendices (NASA CR-3857)
- Vol. V - Space Station Safety Plan (NASA CR-3858)

This document is a precursor to space station safety planning. The document is structured to form a basis for safety planning throughout the life of the Space Station Program.

TABLE OF CONTENTS

	<u>PAGE</u>
INTRODUCTION	1
SCOPE	3
SAFETY PLAN ADMINISTRATION	5
APPENDIX AA - DESIGNATED SAFETY MANAGER ROSTER	7
APPENDIX AB - ORIENTATION BRIEFING	9
APPENDIX AC - SAFETY WORKING GOUPS, BOARDS AND REVIEWS	29
APPENDIX AD - SAFETY PLAN CHANGE PROCEDURES	31
APPENDIX AE - CURRENT SAFETY SUMMARY	33
APPENDIX AF - SAFETY ASSESSMENT PROCEDURE	35
SAFETY OPERATING INSTRUCTION	37
APPENDIX AG - SPACE STATION PROGRAM INCREMENTS	53
APPENDIX BA - APPLICABLE DOCUMENTS	67
APPENDIX BB - PRELIMINARY SPACE STATION CREW SAFETY THREAT LIST	69
APPENDIX BC - SPACE STATION CREW SAFETY CRITERIA	77
APPENDIX BD - SPACE STATION CREW SAFETY GUIDELINES	85
APPENDIX BE - SPACE STATION HAZARD LIST	103

LIST OF FIGURES

SAFETY PLAN

	<u>PAGE</u>
FIGURE 1 - SAFETY PLAN PARTS AND APPLICATION	2
FIGURE 2 - RISK ASSESSMENT PROCESS	4

LIST OF TABLES
SAFETY PLAN

	<u>PAGE</u>
TABLE 1 - TYPICAL THREATS	40
TABLE 2 - SUMMARY OF SAFETY REVIEW PROCESS	42

SPACE STATION SAFETY PLAN

INTRODUCTION

The United States Space Station Program, whose objective is to place a permanent manned presence in low earth orbit by the 1990's, is dedicated to the most cost effective application of the national resources. The objective of the Space Station Safety Program, in support of this national goal, is to ensure its achievement with minimum exposure of the space station assets and personnel to unwarranted risk. The safety program's approach is to realize minimum risk exposure without levying undue design and operational constraints. This will be accomplished by synergistically working within the design and operational planning communities and achieve the safest long-term space station program operations possible with the lowest resource commitment. Implementing this approach will include early specification of safety criteria and requirement through preliminary safety assessments. This will ensure early identification of safety issues and avoid costly subsequent program adjustments.

SAFETY PHILOSOPHY

A safety philosophy states the level of safety desired.

The Space Station safety philosophy is to ensure that no damage to the Space Station or injury to the crew will cause a suspension of operations.

This level of safety is bracketed by 1) allowing no damage to the Space Station and no injury to the crew - a desirable but costly approach, and by 2) crew survival at the expense of the Space Station. The latter implies evacuation and rescue as a minimum. A safety philosophy that requires a level of safety which will normally allow continued operations is a reasonable trade-off between accepting no risk and station abandonment.

PLAN DEFINITION

The Space Station Safety Plan is a management tool to be used by the entire Space Station community - and those who will be directly or indirectly involved - to identify and disposition risks associated with the definition, development, phase-in, build-up and operations of the Space Station. Figure 1 identifies each of the Plan parts and their application.

PURPOSE

The purpose of the Space Station Safety Plan is to ensure that safety impacting contingencies that may arise throughout the life of the Space Station are identified, or will be identified, and ensuring that planning precedes that related increment of the Space Station Program is implemented.

This plan will be constantly changing in order to address the most recent data and to update the next Space Station program increment prior to its implementation. Toward this end, this plan contains administrative and data appendices that will allow the safety community to effect changes to optimize this document's effectiveness as a safety management (DSM's) development and implementation tool.

<u>SECTION</u>	<u>QUESTIONS ANSWERED</u>
<div style="border: 1px solid black; padding: 5px; text-align: center;"> PLAN BODY </div>	<ul style="list-style-type: none"> • WHY A SAFETY PLAN? • WHAT DOES IT DO?
<div style="border: 1px solid black; padding: 5px; text-align: center;"> ADMINISTRATIVE APPENDICES </div>	<ul style="list-style-type: none"> • HOW IS THE PLAN MAINTAINED? • WHO COMPRISES THE SPACE STATION SAFETY TEAM? • WHAT ARE THE PROGRAM REQUIREMENTS? • HOW CAN THE SAFETY PROGRAM GOALS/OBJECTIVES BE DISSEMINATED? • HOW IS A SAFETY ASSESSMENT TO BE DONE? • WHAT IS THE SAFETY PROGRAMS CURRENT STATUS? • WHAT ARE THE SAFETY PLAN TASKS?
<div style="border: 1px solid black; padding: 5px; text-align: center;"> DATA APPENDICES </div>	<ul style="list-style-type: none"> • WHAT DATA ARE AVAILABLE TO HELP THE DESIGNATED SAFETY MANAGER (DSM) DO HIS JOB?

Figure 1 Safety Plan Parts and Application

SCOPE

This Safety Plan concerns all agencies - government, educational and industry - who are part of the team that defines the Space Station concept, prepares its design requirements, integrates the design, develops operational requirements, manages the development planning, designs, develops, fabricates, tests and prepares for operation and support of the station. Appendix AA lists Space Station Designated Safety Managers. This appendix identifies the players for each specific phase of the program. This appendix, as it is updated, will provide a continuity for the Designated Safety Managers associated with the Space Station during its lifetime.

The plan itself is an advisory document whose safety objectives, during each Space Station program increment, are to be identified. These objectives are defined as safety criteria, safety guidelines and safety design/procedural requirements. If these objectives cannot be achieved readily, it is incumbent upon the related increment Designated Safety Manager to advise the Increment Program Manager of the risks associated with not satisfying these safety objectives within the Program Manager's area of responsibility. Objectives that cannot be resolved should be assessed for risk acceptance, with reasons why the unresolved Safety Objective will not expose the Space Station resources to an unacceptable calamity. These incidents of risk acceptance are to be documented in the plan, as noted. Figure 2, indicates the approach to be used to identify, assess and resolve/accept risks on the Space Station Program.

As the safety plan data are aggregated, the plan becomes a historical file of safety objectives, risks, risk acceptances and safety personnel involved. These data are included in the plan directly or by reference.

SAFETY PLAN APPLICATION

To support plan implementation within the various Space Station jurisdiction, a sample orientation briefing is included (Appendix AB). The responsible Designated Safety Managers (DSM's) can structure this briefing to incorporate the plan objectives and tasks, within the area of responsibility. Additional briefing dates are available from his tier-DSM.

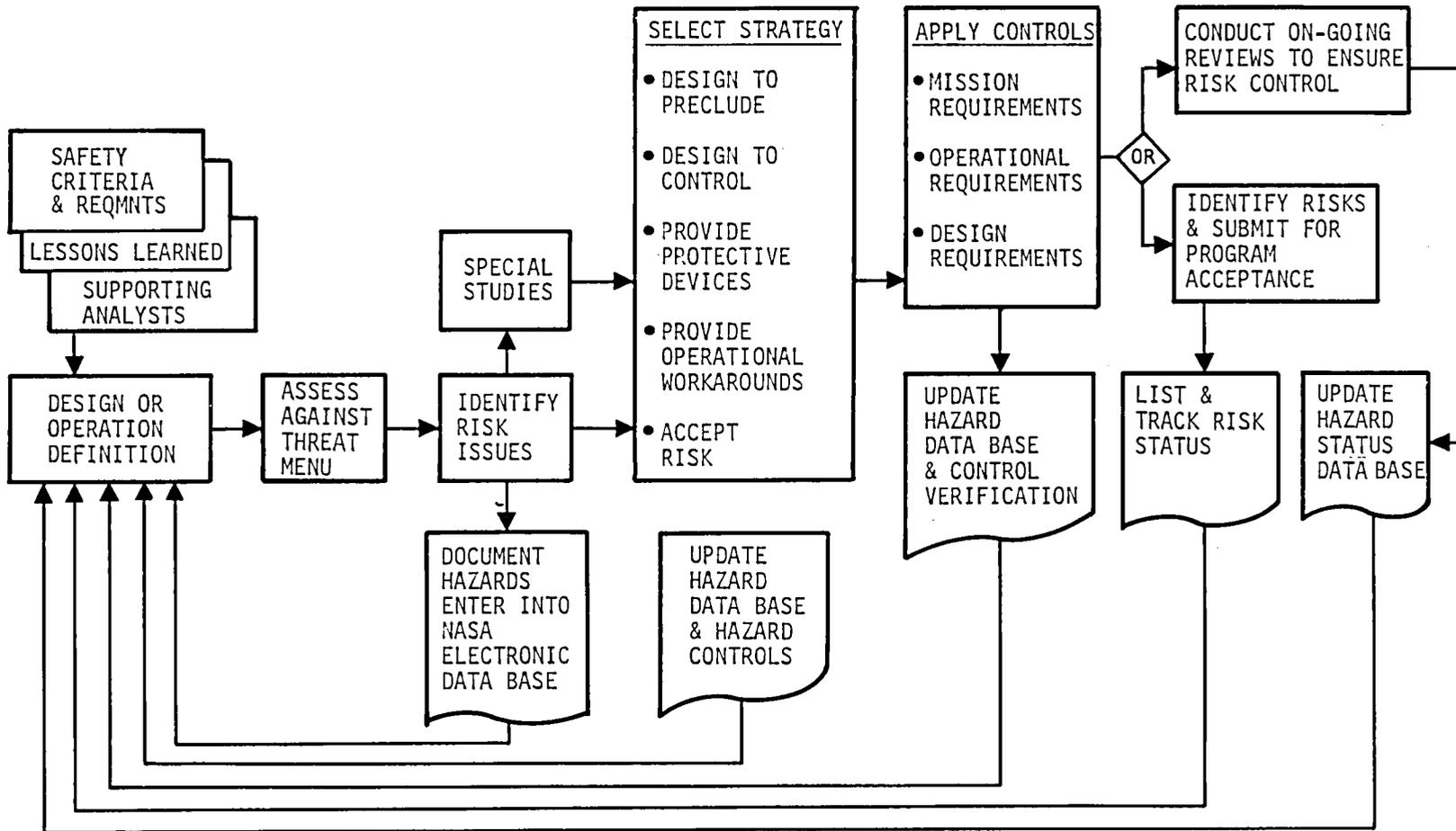


Figure 2 Risk Assessment Process

SAFETY PLAN ADMINISTRATION

Administration of the plan and its task coordination is expanded in Appendices AC, AD, AE and AF.

SAFETY PLAN TASKS

Currently identified plan tasks are listed in Appendix AG. This listing is organized by program increment, identifying safety task products. Updating of this appendix is shared by all program Designated Safety Managers.

SAFETY PLAN SUPPORTING DATA

The "B" series data appendices are to provide a common and current safety data base for each Designated Safety Manager for application within his area of responsibility. Supporting data appendices will be added as required.

This Page Intentionally Left Blank

Appendix AA
DESIGNATED SAFETY MANAGER ROSTER

A centralized safety organization clearly identifiable within the management structure shall be established to assure that all safety activities have timely planning, implementation and effective technical safety management. A Designated Safety Manager (DSM) shall be appointed to manage the safety program and coordinate with other functional organizations on matters related to program safety.

This appendix is to insure all DSM's are identified, together with all pertinent information, to assure an integrated coordination of effort and program documentation.

The following information is recommended as a baseline for all DSM's assigned to the Space Station Program.

- o DSM's Name and Title
- o Organization Represented
- o Organization's Address and Phone Number
- o Department Number and Mail Code
- o DSM's Home Address and Phone Number
- o DSM's Agency/Contractural Area of Responsibility
- o DSM's Background Synopsis and Credentials

This Page Intentionally Left Blank

Appendix AB
ORIENTATION BRIEFING

It shall be within the Designated Safety Manager's (DSM) area of responsibility to advise the responsible management of the obligations and objectives of the Space Station's program. To insure these aspects have been addressed, a "Space Station Safety Program Orientation Briefing" should be prepared and maintained current for the DSM's area of responsibility. An up-to-date copy of this briefing should not only be made available to management within his area of responsibility, but also to his upper tier Designated Safety Manager.

The pages that follow include suggested briefing charts that may be incorporated in the subject Orientation Briefing. The minimum objectives of this briefing should include the following:

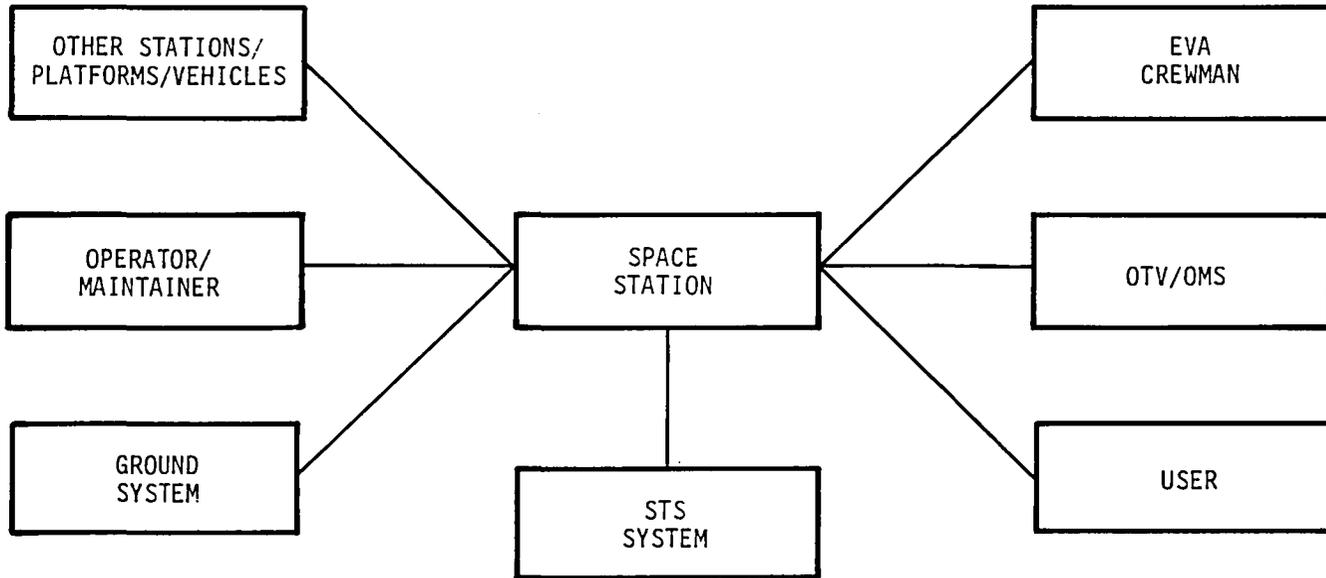
1. Define the scope and philosophy of the Space Station Safety Program.
2. Define the scope of the Space Station organization to illustrate the safety infrastructure.
3. Identify to management their safety responsibilities within the community (agency/corporate).
4. Define how the Space Station safety objectives can be achieved within the designated area of responsibility.
5. Interpret the safety community administrative and tracking systems.

SPACE STATION SAFETY PLAN

ORIENTATION BRIEFING

EXAMPLE

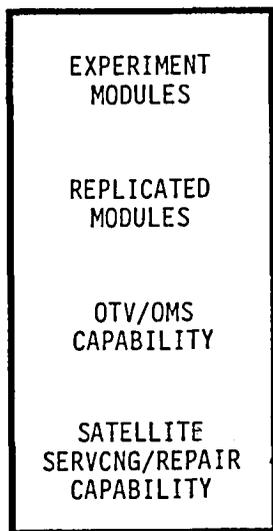
SPACE STATION INTERFACE DEFINITION
ASSUMED PROGRAM ELEMENTS



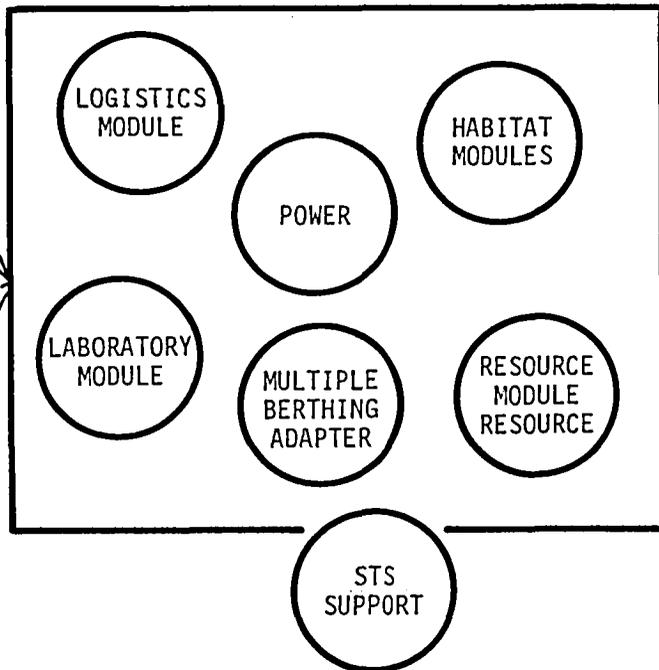
- SAFETY ASSESSMENT AT EACH INTERFACE REQUIRED

SPACE STATION DEFINITION
ASSUMED ARCHITECTURE

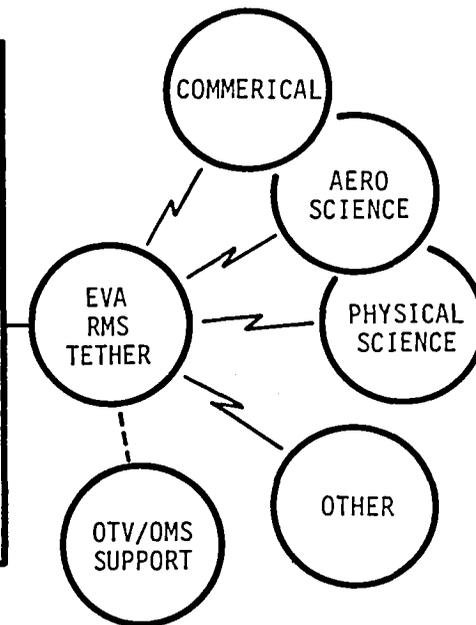
GROWTH ELEMENTS



STATION ELEMENTS



UNMANNED PLATFORMS



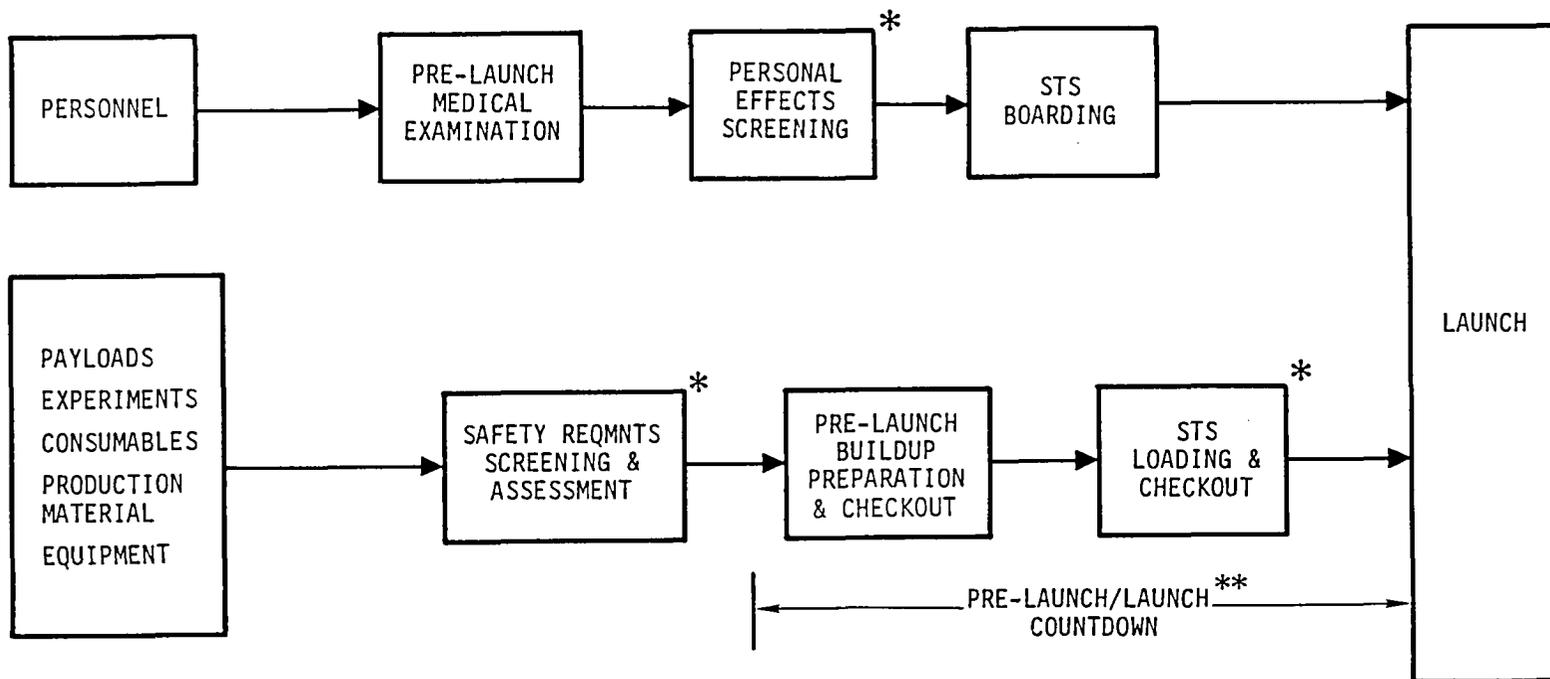
12

- SAFETY ASSESSMENT OF EACH SUB-ELEMENT & THE INTEGRATED SYSTEM REQUIRED

PROGRAM SCHEDULE

EXAMPLE

PRE-LAUNCH PROCESSING AND LAUNCH OPERATIONS
SAFETY ISSUES



14

* NHB1700.7A STS PAYLOAD SAFETY REQUIREMENTS & NHB XXXXXX SPACE STATION SAFETY REQUIREMENTS

** PROCEDURES SCREENING

SPACE STATION BUILDUP SAFETY ISSUES

GROWTH SEQUENCE ELEMENTS (TYPICAL)

1. MODULE MOCK-UP DESIGN/FABRICATION
 2. MODULE DESIGN/FABRICATION
 3. MODULE CHECKOUT
 4. DYNAMIC MOCK-UP (FIT, FORM, FUNCTION TEST)
 5. PAYLOAD ELEMENT PREP, BUILDUP, CHECKOUT
 6. PAYLOAD ELEMENT/STS MATE, LAUNCH, PARK
 7. PAYLOAD ELEMENT-TO-SPACE STATION
STRUCTURAL INTEGRATION
 8. NEW/MODIFIED ELEMENT/MODULE CHECKOUT
 9. INTEGRATED SPACE STATION CHECKOUT
-
- A. ON-GOING STS-TO-STATION LOGISTICS
 - B. SPACE STATION REFURBISHING/UPGRADING



SAFETY ISSUES DEVELOPED THROUGH
ASSESSMENT OF THE THREAT MENU
AGAINST EACH GROWTH ELEMENT
EQUIPMENT & PROCEDURES

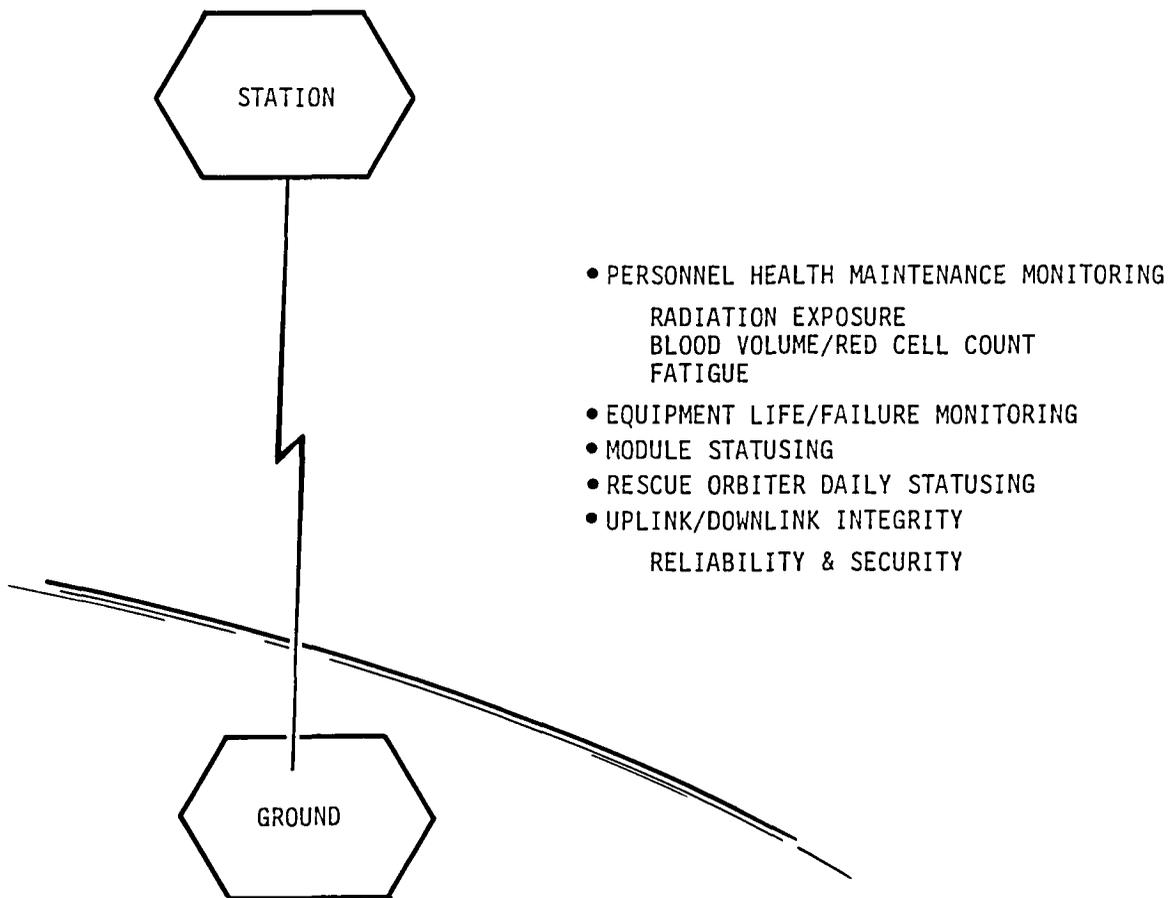
ON-ORBIT OPERATIONS
SPACE STATION OPERATIONS/MAINTENANCE - SAFETY ISSUES

- 0 OPERATIONAL PROCEDURES INTEGRITY SAMPLING
- 0 NORMAL-TO-CONTINGENCY-TO-EMERGENCY OPERATIONS CRITERIA DEFINITION
- 0 MAINTENANCE TASKS DEVELOPMENT SCREENING
 - TOOLS
 - EVA/IVA vs. SHIRTSLEEVE
 - CREW HAZARDOUS ENVIRONMENT EXPOSURE
 - MAINTENANCE IMPACT ON SUBSYSTEM FAULT TOLERANCE
 - CONTAMINATION/DECONTAMINATION (CREW/EQUIPMENT)
 - TASK BUY-OFF/COMPLETION MONITORING AND QUALITY CONTROL
 - MAINTENANCE RECORD INTEGRITY
- 0 PERSONNEL HEALTH MONITORING
- 0 SUBSYSTEM/EQUIPMENT PERIODIC/CONTINUOUS STATUS MONITORING
- 0 PHASE-IN OF NEWLY DEvised PROCEDURES

ON-ORBIT OPERATIONS (USERS)
SAFETY ISSUES

- o COMPLIANCE WITH NHB XXXX "SPACE STATION USERS SAFETY REQUIREMENTS"
- o MINIMUM USERS PERSONNEL SPACE STATION ORIENTATION
 - EMERGENCY PROCEDURES FAMILIARIZATION
 - TRAFFIC PATTERNS (INTERNAL/EXTERNAL)
 - ADMINISTRATIVE RULES
 - SPACE STATION HEALTH MAINTENANCE GUIDELINES
 - RECREATION AND OFF-DUTY GUIDELINES
 - EVA/IVA PRECAUTIONS
- o MATERIAL HANDLING AND PROCESSING CONSTRAINTS

REAL-TIME GROUND MONITORING & SUPPORT OPERATIONS
SAFETY ISSUES



LOGISTICS OPERATIONS
SAFETY ISSUES

- 0 MODULE PREPARATION
 - NHB 1700.7A STS USERS SAFETY REQUIREMENTS
 - NHB XXX SPACE STATION USERS SAFETY REQUIREMENTS
- 0 MODULE BUILD-UP & LOADING
 - VOLATILE/HAZARDOUS MATERIAL HANDLING
 - DISCRETE PARCEL HANDLING
- 0 STS TRANSIT
 - VOLATILES CONTAINMENT/VENTING/PURGE
- 0 MODULE ORBITAL TRANSFER & ATTACHMENT/CONNECTION
 - MATING/CONNECTOR INTEGRITY CHECKOUT
- 0 MATERIAL TRANSFER
 - FLUIDS/BULK OR DISCRETE PARCEL HANDLING
 - FLUIDS/BULK OR DISCRETE PARCEL STORAGE/SECURING
- 0 MODULE LOADING IN STS
- 0 EQUIPMENT/MATERIAL INVENTORY CONTROL
 - MATERIAL QUANTITIES
 - MATERIAL/EQUIPMENT/SPARES LOCATOR CAPABILITY
 - MATERIAL SYNERGY ISSUES - ISOLATED STORAGE REQUIREMENTS, ETC.
- 0 MODULE STS RETURN VS. REFURBISHMENT IN ORBIT



SCREENING

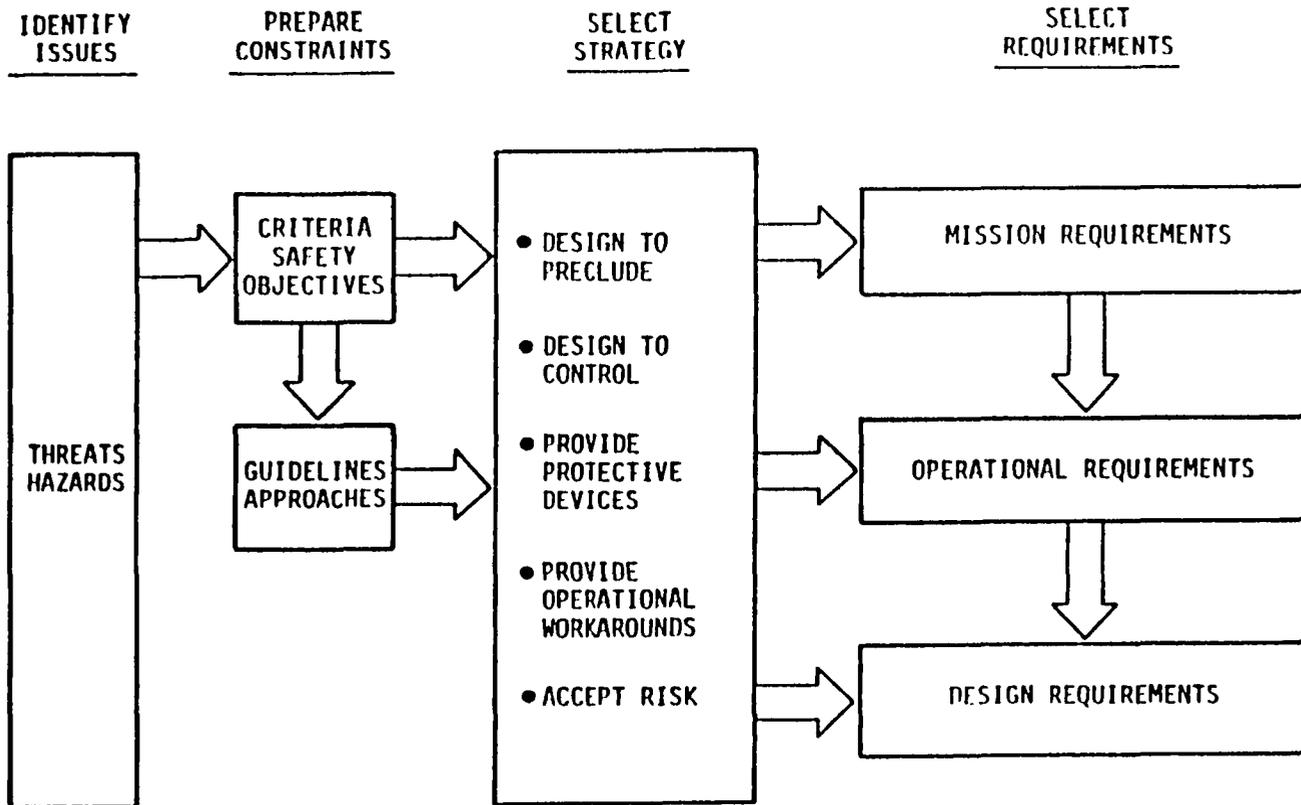
SPACE STATION SAFETY APPROACH

SPACE STATION SAFETY PHILOSOPHY PRECEDENCE
(HOW MUCH SAFETY?)

21

CURRENT OPTIONS	COMMENTS
<ul style="list-style-type: none"> • CAUSE NO DAMAGE WHATSOEVER TO SPACE STATION AND NO INJURY TO CREW • CAUSE NO DAMAGE TO SPACE STATION BEYOND ROUTINE MAINTENANCE CAPABILITY 	<p>DESIRABLE: COST TRADE</p> <p>COST TRADE</p>
<ul style="list-style-type: none"> • CAUSE NO DAMAGE TO SPACE STATION OR INJURY TO CREW WHICH WILL RESULT IN A SUSPENSION OF OPERATIONS 	<p>BASELINE PHILOSOPHY</p>
<ul style="list-style-type: none"> • SPACE STATION REPAIRABLE AND OPERATIONAL WITHIN A SPECIFIED PERIOD OF TIME • CREW SURVIVAL AT EXPENSE OF THE SPACE STATION 	<p>MAY REQUIRE ESCAPE/RESCUE</p> <p>IMPLIES EVACUATION AND RESCUE. AS A MINIMUM</p>

THREAT REDUCTION STRATEGY LOGIC



ANATOMY OF A THREAT

DEFINITIONS:

- THREAT: SITUATION WHICH ENDANGERS EITHER THE CREW OR THE SPACE STATION
- POTENTIAL THREAT: THREATS WHICH MIGHT ARISE, WITHOUT REGARD TO PROBABILITY, FREQUENCY, OR SEVERITY
- POTENTIAL HAZARDS: THREATS WHICH HAVE BEEN DETERMINED TO HAVE A COMBINATION OF PROBABILITY, FREQUENCY AND/OR SEVERITY FOR A GIVEN SCENARIO & WHICH MUST BE DEALT WITH

COMPONENTS OF A THREAT

- CONFIGURATION-ORIENTED HAZARDS
 - MISSION SCENARIO
 - OPERATIONAL MODE
-

TYPICAL SPACE STATION CREW SAFETY
THREAT LIST

- FIRE
 - LEAKAGE
 - TUMBLING/LOSS OF CONTROL
 - BIOLOGICAL OR TOXIC CONTAMINATION
 - INJURY/ILLNESS
 - GRAZING/COLLISION
 - CORROSION
 - MECHANICAL DAMAGE
 - EXPLOSION
 - LOSS OF PRESSURIZATION
 - RADIATION
 - OUT-OF-CONTROL IVA/EVA ASTRONAUT
 - INADVERTENT OPERATIONS
 - LACK OF CREW COORDINATION
 - ABANDONMENT OF SPACE STATION
 - METEOROID PENETRATION
 - STORES/CONSUMABLES DEPLETION
 - STRUCTURAL EROSION
 - ORBIT DECAY
 - LOSS OF ACCESS TO A HATCH
 - TEMPERATURE EXTREMES
 - DEBRIS
-

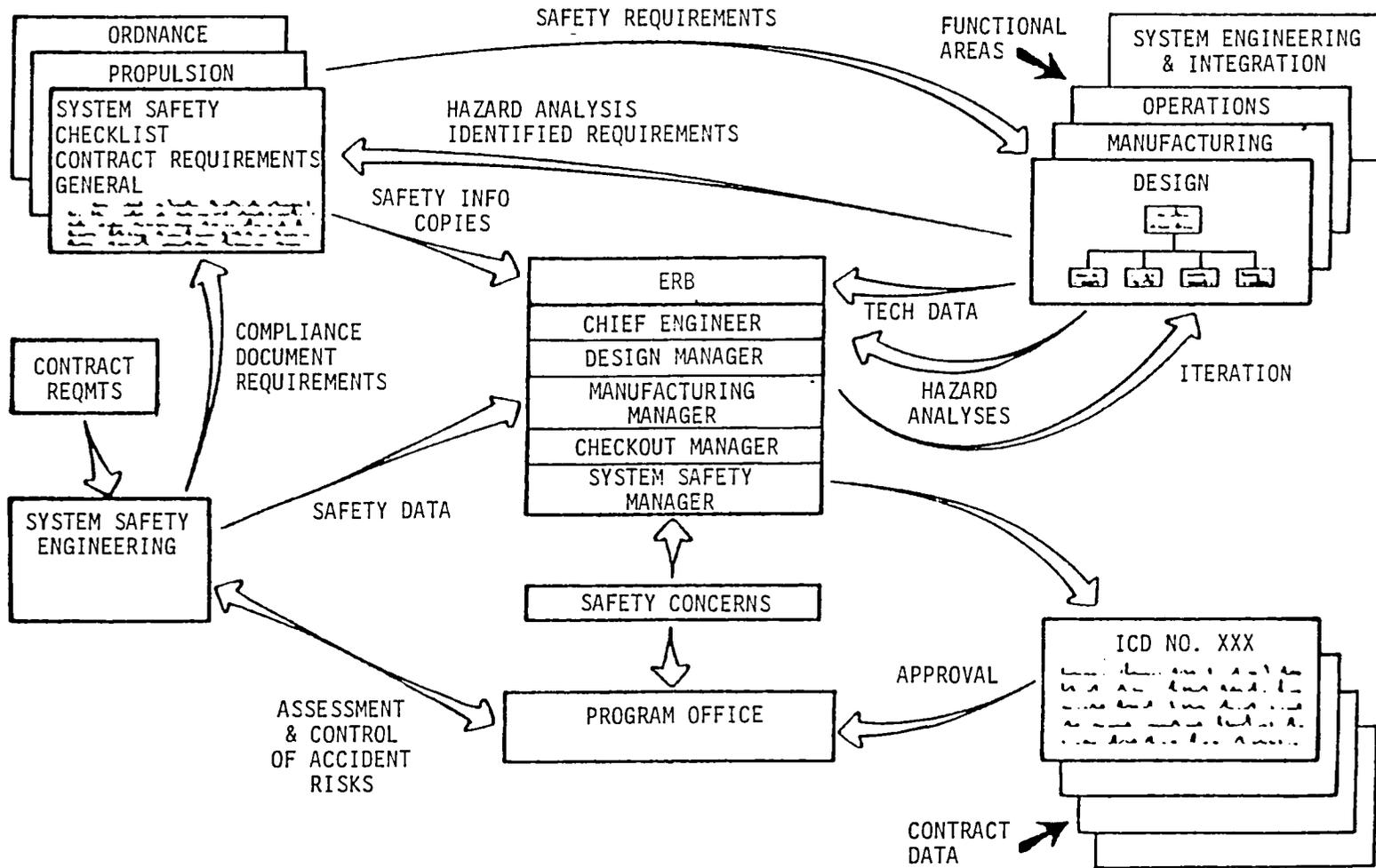
THREAT ASSESSMENT - TYPICAL

THREAT	CAUSATIVE FACTORS	STRATEGY(IES)
<p>FIRE</p>	<p>GROUND & SPACE HABITABLE AREAS • FUEL/OXIDIZER/IGNITION SOURCES COEXIST</p> <p>SPACE NONHABITABLE AREAS • FUEL/OXIDIZER/IGNITION SOURCES/ TEMPERATURE/PRESSURE COEXIST</p> <p>• CATALYTIC REACTION</p> <p>• CHEMICAL REACTION</p> <p>• IGNITION SOURCES (ELECTRICAL/ELECTROSTATIC)</p>	<p>1. EXCLUDE TWO OF THE THREE ELEMENTS 2. WHEN TWO ELEMENTS ARE PRESENT, INERT 3. MATERIALS CONTROLS</p> <p>1. EXCLUDE THREE OF THE FIVE ELEMENTS 2. MATERIALS CONTROL</p> <p>1. INERT ENVIRONMENT 2. CONTROL SURFACE TEMPERATURE 3. MATERIALS CONTROL</p> <p>1. INERT ENVIRONMENT 2. MATERIALS CONTROLS 3. EXTINGUISHING AGENTS</p> <p>1. PROPER GROUNDING/BONDING 2. WIRING CONTROLS 3. PROPER CIRCUIT PROTECTION 4. ISOLATION OF CIRCUITS FROM COMBUSTIBLE MATERIALS 5. MATERIAL SELECTION</p>

THREAT ASSESSMENT - TYPICAL

THREAT	CAUSATIVE FACTORS	STRATEGY(IES)
CONTAMINATION (TOXIC)	MATERIALS OUTGASSING	<ol style="list-style-type: none"> 1. LIST OF PROHIBITED MATERIALS FOR USE IN SPACE STATION HABITABLE AREAS 2. REAL-TIME 3-D LOCATION MAPPING OF ALL MATERIALS ONBOARD VEHICLE <ul style="list-style-type: none"> • MASS • AREA 3. LISTING OF TOXINS GENERATED BY FABRICATION/REPAIR PROCESSES STORED & COMPARED TO CONTAMINATION MONITORING DATA 4. REAL-TIME CONTAMINATION MONITORING SYSTEM
(PARTICULANTS)	SPILLS/LEAKAGE	<ol style="list-style-type: none"> 1. EXCLUDE HAZARDOUS FLUIDS FROM CREW/HABITATS 2. REAL-TIME CONTAMINATION MONITORING SYSTEM 3. CONTAINMENT/CLEANUP
(BIOLOGICAL)	FREE MATERIAL <ol style="list-style-type: none"> 1. EXPERIMENTS 2. BACTERIAL AGENTS INTRODUCED TO HABITAT (WASTE MANAGEMENT) 3. BODY GROWTH OF BACTERIA DUE TO ABSENCE OF CONVECTION COOLING 	<ol style="list-style-type: none"> 1. FILTRATION 2. ELECTROSTATIC PRECIPITATION 1. FAIL-SAFE DESIGNS 2. GERMICIDAL AGENTS 3. MATERIAL SELECTION

XXXXXX SAFETY PROGRAM – SPACE STATION
FUNCTIONAL ADMINISTRATION



This Page Intentionally Left Blank

Appendix AC
SAFETY WORKING GROUPS, BOARDS AND REVIEWS

The System safety organizations will support and/or participate in the Space Station Inter-Center System Safety Working Groups, the Senior Safety Review Board, Program Milestone Reviews, Program Management Safety Reviews, and Safety Program Review activities.

- a. Inter-Center System Safety Working Group Meetings. The authority, purpose, membership, and responsibilities of the Inter-Center System Safety Working Group are defined in (TBD). The Group will convene on a periodic basis to (1) maintain cognizance of system safety activities (2) maintain safety communications channels throughout the various system safety activities and (3) review hazard status. Meetings will be scheduled and planned by the Space Station Program Safety Manager consistent with program activities status and milestone schedules.
- b. Senior Safety Review Board Meetings. The Senior Safety Review Board purpose, scope, policy, responsibility, membership, and procedures are defined in (TBD). Support to the Board will be required from Safety Managers to review open hazards and closure rationale for accepted risks.
- c. Program Milestone Reviews. Risk management data will be provided in accordance with IRL/IRD. These data shall be based on efforts such as hazard analyses, failure modes and effects analyses, human factors analyses, and interface analyses. These data shall be presented in adequate detail to allow a management decision as to readiness to proceed, from a safety viewpoint, with the next program phase or with planned test, flight, or on-orbit operation.
- d. Readiness Inspections. The Safety organization shall participate in readiness inspections prior to performing any operation or test which is potentially hazardous to personnel or hardware, has a high risk in terms of program success, or involves hardware, facilities, or effort of significant expense. A safety assessment shall be made of facilities, test articles, procedures, and personnel training, experience, certification, and management. The Safety activity also includes an assessment of previous test or operations data and visual inspection of the operational configuration.

The results of readiness inspections will be required for presentation at program milestone reviews if the operation is related to a program master schedule milestone.

- e. Program Management Safety Reviews. The safety organizations shall support program management safety reviews which will be presented as agenda items at the program or project change control boards. Safety will advise management of open hazards, the actions being implemented to resolve the hazards, the organization responsible for the actions, and the expected date of resolution. The reviews will include descriptions of new risks that have been identified and the proposed risk acceptance rationale.

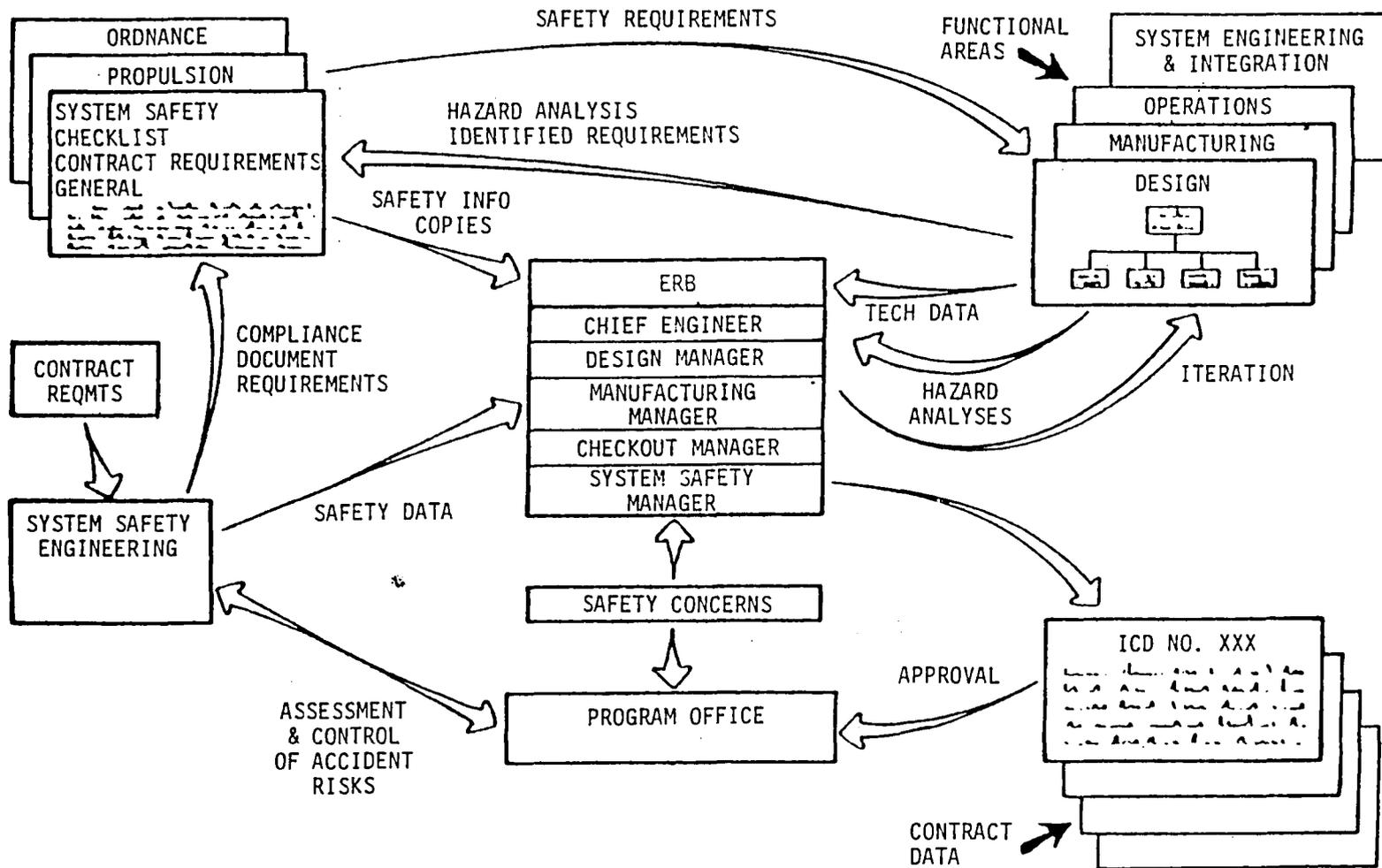
- f. Safety Program Reviews. Safety review teams, which may consist of Headquarters, program, or project personnel, will periodically review safety organizations, programs, and activities. The safety organizations shall provide data consistent with the depth of review to be conducted, and will verify internal compliance and the compliance with system and occupational safety and health safety requirements. A schedule of reviews shall be established at least 1 year in advance of the review and a file of the review results shall be maintained for review. Participation by NASA in contractor and subcontractor safety reviews will be at the discretion of NASA.

(Extracted from "Safety, Reliability, Maintainability and Quality Provisions for the Space Station Program", 1D200, para. 5.)

Appendix AD
SAFETY PLAN CHANGE PROCEDURES

The Designated Safety Manager (DSM) shall evaluate all changes, waivers, deviations and any additional hazards identified during this change process. Processing of Safety Plan changes will conform to the closed loop system of hazard reporting, data storage and the approved feedback of corrective action. This system shall be developed, implemented and maintained as noted in the basic flow chart, page AD-2. This procedure shall provide changes to hazard data and summary information as specified in the approved and applicable documents. The data elements and formats shall be consistent with Space Station Information System Requirements. This information system will also be utilized for maintaining hazard information and to provide the capability of accomplishing a complete hazards assessment. The Designated Safety Manager (DSM) shall be responsible for assuring complete and timely hazard change reporting and all entries into the electronic network safety data base at the time of identification and approval.

XXXXXX SAFETY PROGRAM – SPACE STATION
FUNCTIONAL ADMINISTRATION



32

Appendix AE
CURRENT SAFETY SUMMARY

The Designated Safety Manager (DSM) will provide a monthly safety summary to his tier-DSM according to the Information Requirements Description (IRD) of the contract. The purpose of the monthly safety summary is to initiate the following:

1. Alert the community to any safety problems requiring inter-agency coordination. A suggested outline for the report (as further definitized by the contract IRD) could include:
 - a. Contract milestones: completion of preparation for related status.
 - b. Risk issues.
 - c. Projected activities.
 - d. Safety program issues.
2. Indicate safety issues that may be schedule/cost risk drivers.
3. Incrementally update the Space Station electronics network data base (safety analyses/trade studies).
4. This Appendix can provide a data file for the DSM's monthly safety summaries.

This Page Intentionally Left Blank

Appendix AF
SAFETY ASSESSMENT PROCEDURE

The method whereby the Designated Safety Manager (DSM) ensures the conduct for safety assessment of hardware, software and operations/procedures, is to be included in this appendix. An updated copy of these data will also be forwarded to his tier-DSM. A suggested procedure is enclosed. This may be expanded or modified to satisfy the risk assessment needs within a DSM's area of responsibility. JSC Form ZZZ "Space Station Hazard Report" is included to encourage uniformity in hazard reporting. Effort has been initiated to assure this report formatting is included in the Space Station electronic network Safety Data Base.

EXAMPLE

SPACE STATION SAFETY
DEPARTMENT INSTRUCTION

MODULE/SYSTEM HAZARD ANALYSIS PROCEDURE

SAFETY OPERATING INSTRUCTION
MODULE/SYSTEM HAZARD ANALYSIS PROCEDURE

1.0 PURPOSE

The purpose of this Safety Operating Instruction is to define the procedure to be used in preparing safety assessment reports. This Safety Operating Instruction further defines a safety analysis and safety reviews in support of which the safety assessment reports are prepared.

2.0 SCOPE

This Safety Operating Instruction applies to a system safety engineer of XXXX Company for in-house processing of payload hazards associated with the Space Station (SS). This Safety Operating Instruction is based on NHBXXX "Safety Requirements for Space Station Users, Experimenters and Interfacing Vehicles and Hardware". Also the noncompliance report instruction is included in this Safety Operating Instruction for the cases in which a safety requirement cannot be met.

3.0 PROCEDURE

3.1 OVERVIEW

The following statement describes how a safety analysis, a safety assessment report, and a safety review are interrelated:

In support of a safety review, a safety engineer prepares a safety assessment report which documents the results of a safety analysis performed by him/her.

In order to facilitate understanding of this interrelationship, this section defines and further describes hazards, safety analyses, and safety reviews.

3.1.1 THREATS AND HAZARD LEVELS

Although there may be many secondary or contributory hazards, threats are identified as the primary concerns applicable to the Module/System. Table 1 contains a selected list of the threats and their descriptions.

During the analytical process to identify hazards, a safety engineer should attempt to define the hazards in terms of these threats. A difficulty common to all such lists is that there is a considerable overlap between the threats, and assignment of an unsafe act or condition to any one hazard group is arbitrary. What is important is that potentially hazardous items or conditions are identified, described, and tracked through the safety review process. Events or conditions that affect the success of a Space Station's mission or cause loss or damage to payload hardware are not hazards unless such events or conditions result in a risk to the SS or personnel.

Hazards are also classified with respect to potential as hazard levels. There are two hazard levels. One is a critical hazard which results in damage to the SS equipment or the use of contingency or emergency procedures. A catastrophic hazard is the other level which results in the potential for loss of life or major injury which results in the incapacitation of the crew or loss of the module, ground facilities, or SS equipment.

3.1.2 SAFETY ANALYSIS

A safety analysis is a technique used to systematically identify, evaluate, and resolve hazards. In order to identify the hazards applicable to a module/system or its GSE, a safety engineer shall conduct safety analyses both at the system and subsystem levels. Typically such analyses assess the entire system and its interface or each of the subsystems and their interfaces against a list of the hazard groups shown in Table 1. In addition, each system and subsystem shall be evaluated to determine the applicability of all the technical safety requirements of NHB 1700.7A and KHB 1700.7. A safety engineer may use the fifteen subsystems listed and defined in JSC 11123 to conduct the safety analyses. However, the selection of subsystem groupings are arbitrary, and any convenient grouping may be used.

It is the responsibility of a safety engineer to conduct a safety analysis early in the design of the module/system/GSE and to update that analysis as necessary as the design matures.

TABLE 1 TYPICAL THREATS

THREAT	DESCRIPTION
Collision	hazards which occur where module/system elements are allowed to break loose and impact SS structure, other payloads, or flight and ground personnel
Contamination	hazards associated with the release of toxic flammable, corrosive, condensible, or particulate matter
Corrosion	hazards resulting from the structural degradation of metallic and nonmetallic equipment
Electrical Shock	hazards responsible for personnel injury or fatality because of electrical current passing through any portion of the body
Explosion	hazards resulting from the violent release of energy as a result of module/system element overpressurization, fire, chemical reaction, excessive temperature, malfunctioning equipment or structural failure causing the release and collision of equipment with other structures
Fire	hazards associated with the rapid oxidation of module/system element combustibles
Injury and Illness	hazards capable of inflicting physical injuries or illness of any sort on one flight or ground crews during all mission phases
Loss of Module	hazards which could degrade the structural, and thermodynamic integrity of the space station.
Radiation	hazards associated with the exposure of the human body and sensitive control equipment to ionizing radiation, ultraviolet or infrared light, laser, and electromagnetic or RF (radio frequency) generating equipment
Temperature Extremes	hazards associated with the departure of temperature from normal

3.1.3 SAFETY REVIEWS

Four safety reviews (Phases 0, I, II, and III) are normally conducted for both module/system design and flight operations and for Ground Support Equipment (GSE) design and ground operations. The four safety reviews are conducted by the safety review panels at JSC, the SS flight operator, and at KSC, the SS launch/landing site operator.

The common objectives of these safety reviews are to assess the safety of each SS module/system, its associated GSE, and ground operations and to assess compliance with the requirements of NHB XXX, NHB 1700.7A and KHB 1700.7.

The Phase 0 safety reviews are informal meetings chaired by a JSC safety representative for module/system design and flight operations and a KSC safety representative for GSE design and ground operations. The Phase I through Phase III safety reviews are formal reviews conducted by the safety review panels. During the formal reviews, a safety engineer should give a presentation which includes a brief description of the module/system/GSE and its operations, followed by data unique to the phase being reviewed.

The timing, objectives, and safety tasks for each of the safety reviews are summarized in Table 2.

TABLE 2 SUMMARY OF SAFETY REVIEW PROCESS

PHASE	TIMING	SAFETY EFFORTS	PURPOSE OF REVIEW
0	Module/System/GSE conceptual design established	<ol style="list-style-type: none"> 1. Perform preliminary safety analysis. 2. Prepare a ground operations concept (KSC). 	<ol style="list-style-type: none"> 1. Identify potential hazards and applicable safety requirements.
I	Module/System/GSE preliminary design established	<ol style="list-style-type: none"> 1. Define and expand safety analysis to reflect the preliminary design: <ol style="list-style-type: none"> a. Define hazards. b. Define hazard causes. c. Evaluate actions for reducing or controlling hazards. d. Identify approach for safety verification. 2. Prepare a mission (or ground operations) scenario. 3. Determine compliance with NHB 1700.7 and KHB 1700.7. 	<ol style="list-style-type: none"> 1. Assess the preliminary design against NHB 1700.7 and KHB 1700.7. 2. Evaluate preliminary hazard controls and safety verification methods.
II	Module/System GSE final design established	<ol style="list-style-type: none"> 1. Refine and expand safety analysis. <ol style="list-style-type: none"> a. Evaluate interfaces and mission (or ground operations) procedures, plans and timelines. b. Update hazard descriptions, causes, and controls. c. Finalize test plans, analysis procedures, or inspections for safety verification. 2. Finalize description of ground operations flow. 3. Determine compliance with NHB 1700.7 and KHB 1700.7. 	<ol style="list-style-type: none"> 1. Assess final design against NHB 1700.7 and KHB 1700.7. 2. Concur on specific hazard controls and safety verification methods.
III	Module/System GSE fabrication and testing complete.	<ol style="list-style-type: none"> 1. Complete safety analysis. 2. Prepare safety assessment report. 3. Complete all safety verification tests, analyses and/or inspections. 4. Prepare safety compliance data package. 	<ol style="list-style-type: none"> 1. Approval of safety assessment report. 2. Review of safety compliance data package. 3. Identify open safety items.

3.2 SAFETY ASSESSMENT REPORTS

A safety assessment report documents the result of a safety analysis performed by a safety engineer. The safety assessment report is then maintained and submitted by the safety engineer to the module/system safety review panels approximately 45 days prior to each safety review. The safety assessment report generally contains the following:

- (1) Descriptions of the module/system/GSE and its safety-critical subsystems. A safety-critical subsystem is a subsystem containing an element of risk.
- (2) Mission scenario and ground operations description.
- (3) Requirements matrix.
- (4) Hazard reports.
- (5) Other data specifically required for each safety review.

Instructions for completion of a hazard report and a requirements matrix are shown along with their forms in Appendix A and B of JSC 1380A, respectively. The requirements matrix (JSC Form 000, SS Module/System Safety Requirements Applicability Matrix) contains the assessment of the applicability of the technical requirements of NHB 1700.7A with respect to each module/system element. From a safety view point, the hazard reports constitute the most important element of the safety assessment report.

Through the safety analysis, the safety engineer evaluates each identified hazard for means of eliminating, reducing, or controlling the hazard. The safety engineer also identifies the approach for verifying compliance with the safety requirements. Then the safety engineer documents the results of this effort in a hazard report (JSC Form ZZZ, Hazard Report).

Among the data specifically required for each safety review is Ionizing Radiation Source Data Sheet (JSC Form 44 (Revision 10-81)). The Ionizing Radiation Source Sheet provides the information which will satisfy the initial JSC and KSC data requirements for radioisotope sources and radiation-producing equipment. Paragraph 5.3.3 of JSC 13830A provides additional information on this Ionizing Radiation Source Data Sheet.

3.2 SAFETY ASSESSMENT REPORTS (Cont'd)

Detailed data requirements for each safety review are shown in paragraphs 5.2.1, 5.3.1, 5.4.1, 5.5.2 of JSC 13830A. The safety engineer shall satisfy these data requirements in preparing the safety assessment reports.

Up to the Phase II safety review, the safety engineer submits the safety assessment report which contains all the required data to the safety review panels. For the Phase III safety review, the safety engineer submits to the panels a safety compliance data package which includes not only the safety assessment report but also other required data described in paragraph 5.5.2 of JSC 13830A.

3.3 NONCOMPLIANCE REPORT

When a specific safety requirement of NHB 1700.7A or KHB 1700.7 cannot be met, the safety engineer completes a noncompliance report and submits it for disposition.

Prior to the submittal of the noncompliance report, the safety engineer must develop appropriate rationale which defines the design features and/or procedures used to conclude that the noncompliance condition is safe. All noncompliance reports should be coordinated with the appropriate NASA center prior to submittal and should be submitted as soon as it is determined that the safety requirement cannot be met.

A noncompliance report could be approved either as a waiver or as a deviation. A waiver is approved for a single mission while a deviation is approved for more than one mission.

Section 6.0 of JSC 13830A contains more information regarding the noncompliance report, including the addresses to which the noncompliance report shall be submitted.

<u>PHASE</u>	<u>TIME</u>	<u>OBJECTIVES</u>
0	Concept	Identify safety-critical subsystems, groups, hazards, and applicable safety requirements for subsystems and associated ground operations. (A safety-critical subsystem is a subsystem containing an element of risk.)
I	Preliminary Design Review (PDR)	Assess the implementation approach, review hazards and resolution, and develop an understanding of verification approach.
II	Critical Design Review (CDR)	Verify design compliance with requirements, review verification methods.
III	Delivery to Customer	Validate the incorporation of previous safety review agreements, assure the satisfactory completion of safety verification activities, provide agreement that safety activities have been satisfactorily completed.

It is essential for a safety engineer to pursue the above objectives in preparing each safety assessment report.

PROCEDURE

1. Hazard Groups and Levels

Since the identification of the SS module/system hazard is the necessary starting point of a safety analysis, it is strongly needed to define the hazard and hazard levels and to identify the hazard groups.

A hazard is the presence of any potential risk situation caused by an unsafe act or condition. There are numerous potential risk situations associated with the SS module/system which directly or indirectly affect the safety of SS flight or ground personnel. Therefore, it is necessary to identify such hazards to start a safety analysis.

The following data are required for a phase 0 safety review:

- a. Module/System description and operation.
- b. Hardware description of safety-critical subsystems (existing level, new and reflowed). A safety-critical subsystem is a subsystem containing an element of risk.
- c. Completed module/system safety matrix. (Figure 1)
- d. Completed hazard list. (Figure 2)

The module/system description and operation should be of sufficient detail to permit identification of all subsystems, with emphasis on stored energy, which have potential for creating hazards.

3. Phase I Safety Review

During the early design phase, a safety engineer refines and expands the safety analysis by evaluating each hazard for means of eliminating, reducing, or controlling the hazard and by identifying the approach for verifying compliance with the safety requirements. Then the safety engineer documents the results of this effort on a hazard report form (JSC Form ZZZ). Instructions for completion of the hazard report are shown in Figure 3 on page 11.

Each hazard report should stand alone; therefore, it must be supported by data such as block diagrams, schematics, a description of safety-critical subsystems and their operations, and nonmetallic material and radioactive source information. The block diagram or preliminary schematic should indicate the design approach which is intended to control the identified hazard. Partial diagrams and schematics are satisfactory, provided that the element for hazard control is identified.

Preliminary materials safety assessments (addressing flammability, off-gassing, and materials compatibility with hazardous fluids as applicable) should be conducted for the phase I safety review and documented on module/system hazard reports.

The following data, which must be submitted 30 days in advance, are required for the formal presentation at the phase I safety review:

- a. Block diagrams, schematics, and/or a description of safety-critical subsystems and their operations.
- b. Hazard reports.
- c. Module/System assembly and checkout operations to be conducted at KSC, with preliminary timelines.
- d. Radioactive source questionnaire.

In most cases, there are no radioactive sources involved in the module/system hazard analysis. If a safety engineer has to deal with a radioactive source, he/she should use a radioactive source questionnaire (JSC Form 00Z) shown in JSC 13830.

4. Phase II Safety Review

As the module/system and GSE design is completed and refined, a safety engineer further updates and expands the safety analysis. The safety engineer updates the original signed hazard reports completed at phase I to include additional data on control of the hazard causes and safety verification methods.

The following data are required for a phase II safety review:

- a. Safety-critical subsystem descriptions (update).
- b. Engineering drawings of safety-critical subsystems when specifically requested.
- c. Module/System assembly and checkout operations to be conducted at KSC (update).
- d. A list of safety-related failures or accidents.
- e. A list of technical operating procedures related to identified hazard controls and date of availability for review.
- f. Updated hazard reports and support data including the following:
 - (1) A list of equipment generating hazardous radiation.
 - (2) Radioactive source questionnaire (update).

5. Phase III Safety Review

The safety analysis is completed at the time of the phase III safety review. A safety engineer updates and submits the hazard reports completed at phase II for final approval. All the safety compliance data required by the SP&R (Safety Policy and Requirements) document (NHB1700.7A) are submitted for review at this time. The safety assessment report, which is a part of the safety compliance data, includes the completed hazard reports and the identification of any open safety item.

The following data are required for a phase III safety review.

- a. Updates of safety-critical subsystems descriptions.
- b. Updates of safety-critical subsystem engineering drawings when specifically requested.
- c. Results of applicable safety verification tests and analyses.
- d. Safety compliance data as follows:

- 1) A safety assessment report which documents the results of a safety analysis, including hazard description, controls, and safety verification methods (see JSC 13830).
- 2) Approved waivers to safety requirements.
- 3) Radioactive source questionnaire.
- 4) A list which identifies and characterizes all RF transmitters and all electromagnetic radiation which exceeds the limit for cargo-produced radiated fields as specified in JSC 07700, Volume XIV, attachment I. In addition, the list shall include equipment capable of producing a field strength more than 10 milliwatts per square centimeter for ground safety purposes.
- 5) A log book maintained on each pressure vessel/system showing pressurization history, fluid exposures and other pertinent data shall be delivered with the module/system. (For the phase III safety review, a summary of the log book is sufficient.)
- 6) A summary of all safety-related failures or accidents related to module/system processing, test and checkout, including an assessment of their potential impact to SS, elements of SS, and to ground safety, together with action taken to prevent recurrence.

- 7) Detailed technical operating procedures for launch operations which are hazardous in nature. There shall be step-by-step directions covering items such as personnel access controls, emergency procedures, and weather restrictions.
- 8) A list of all uses of mercury and its compounds in accordance with the data requirements of paragraph 209-1b of NHB1700.7A.
- 9) A list of all pyrotechnic initiators installed or to be installed on the module/system, giving the function to be performed, the part number, the lot number, and the serial number.

6. Waivers

When a specific safety requirement cannot be met, a safety engineer completes a waiver request, JSC Form ZZZ. If the waiver request is for flight, the safety engineer submits it to the Manager, SS Operations Office, code PF, JSC; if for GSE and ground operations, to the Director, Safety, R&A, Protection Service, code SF, KSC.

All the waiver requests should be coordinated with the appropriate NASA center prior to submittal and should be formally submitted as soon as is determined that a safety requirement cannot be met. Each waiver request will address only one hazard or hazard cause. After initial coordination, a safety engineer will formally submit the waiver request for approval. The safety engineer will be formally notified of the acceptance or rejection of the waiver request.

Although there may be many secondary or contributory hazards, ten basic hazard groups were identified as the primary concerns applicable to SS module/systems. Table 1 on page 4 contains the list of these hazard groups and their descriptions. These hazard groups also appear on a safety matrix (JSC Form ZZZ) which is required for the phase 0 safety review - see section 2 of Procedure.

Also, hazards are classified according to potential as hazard levels. There are two hazard levels. One is a critical hazard which results in damage to SS equipments, or the use of contingency or emergency procedures. A catastrophic hazard is the other which results in the potential for personnel injury, loss of the Module, ground facilities, or SS equipment.

2. Phase 0 Safety Review

During the concept phase of the module/system and GSE development, a safety engineer performs a preliminary system-level safety analysis in order to determine the hazard groups associated with the module/system subsystem elements and to identify them. Then the safety engineer documents the results of this analysis on a safety matrix (JSC Form 000) and a hazard list (JSC Form ZZZ). Instructions for completion of the safety matrix and hazard list are shown.

SPACE STATION HAZARD REPORT		NO.
SYSTEM/OPERATION		PHASE
SUBSYSTEM	THREAT	DATE
HAZARD TITLE		

APPLICABLE SAFETY REQUIREMENTS:	HAZARD CATEGORY
	CATASTROPHIC
	CRITICAL
DESCRIPTION OF HAZARD:	

HAZARD CAUSES:

HAZARD CONTROLS:

SAFETY VERIFICATION METHODS:

STATUS OF VERIFICATION:

APPROVAL	ORGANIZATION	SS
PHASE I		
PHASE II		
PHASE III		

This Page Intentionally Left Blank

APPENDIX AG

SPACE STATION PROGRAM INCREMENTS

SAFETY PLAN TASKS

(Preliminary)

83

The purpose of this appendix is to identify safety tasks as they relate to the Space Station program development cycle. Additionally, the task's products are identified.

AUGUST 7, 1984

SPACE STATION PROGRAM INCREMENTS/SAFETY PLAN TASKS (APPENDIX AG)

1. REQUIREMENTS DEVELOPMENT

SAFETY TASKS

SAFETY PRODUCTS/INPUTS

Integration

Identify all Space Station program jurisdictional elements and their Designated Safety Managers (Agency & Contractor)

Space Station Safety Plan (Update)

Prepare/Update Safety Plans for all increments/elements identifying specific detail safety tasks per increment

Space Station Safety Sub-Plans Appendix AG (Update)

Mission

Assess mission requirements to identify which criteria are mandated by mission objectives

Safety Criteria Matrix

Identify new hazards/risk issues related to mission requirements

Preliminary Hazard Analysis

Operations

Determine which operations are inherently hazardous

Preliminary Hazard Analysis (Update)

System Design

Assess system requirements to identify which safety criteria are incorporated in initial system specification

Safety Criteria Matrix

Add new design requirements to support safety criteria

Safety Design Guidelines Appendix BD

Human Factors Design

Review Human Productivity Contract data to determine which requirements support safety criteria

Safety Criteria Matrix

Reliability

Determine which stated redundancies support safety criteria

Safety Criteria Matrix

Safety

Develop Safety requirements in addition to those incorporated in the mission, operations, initial system design and reliability requirements

Safety Design Guidelines

Maintainability

Determine if maintainability objectives support precautionary actions required to maintain hazardous systems, or conduct hazardous operations

Safety Criteria Matrix

Material Control

Ensure material screening, inventorying and locating capability of Space Station Material Control System can support the maximum safety allowable levels, both long term and for stated periods of time (8-hrs/day, 1-hr/day, or less)

Space Station Maximum Threshold Level Values; Input to NHB XXY

Safety input into NHBYYY "Space Station Material Handling and Control Requirements and Procedures" (Draft)

2. INTERFACE DEFINITION (STATION-TO-.....)

55

Station

Develop space station safety requirements to be applied to all interfacing elements

NHB XXX "Safety Requirements for Space Station Users, Experimenters and Interfacing Vehicles and Hardware" (Draft)

Shuttle

Apply requirements of NHB1700.7A to space station elements to be transported on STS

Interface Hazard Analysis (Element Interface Analysis Report)

Ground Segment

Apply requirements of KHB1700.7/ SAMTO HB S-100 for KSC/VAFB located Space Station ground equipment and operations

Interface Hazard Analysis (Element Interface Analysis Report)

Operations

Assess procedure/software interfaces to identify hazardous operations

Mission Hazard Analysis

Maintenance

Identify hazardous maintenance activities, including maintenance whose synergistic effects could generate hazardous situations

Mission Hazard Analysis (Input)

Apply requirements of NHB XXX and NHB XXY to all maintenance activities

Interface Hazard Analysis (Element Interface Analysis Report)

Extra Vehicular Activity (EVA)	Identify hazardous EVA activities for input into Mission Hazard Analysis	Mission Hazard Analysis (Input)
	Apply requirements of NHB XXX and NHB XXY to EVA activities, and EVA suit related activities	Interface Hazard Analysis (Element Interface Analysis Report)
Orbital Maneuvering System	Identify critical functions and/or hazardous activities associated with the OMS in concert with the Space Station	Mission Hazard Analysis (Update)
	Apply requirements of NHB XXX and NHB XXY to all OMS/Space Station interfaces	Interface Hazard Analysis (Element Interface Analysis Report)
Orbit Transfer System	Identify critical functions and/or hazardous activities associated with the OTS in conjunction with the Space Station	Mission Hazard Analysis (Update)
	Apply requirements of NHB XXX and NHB XXY to all OTS/Space Station interfaces	Interface Hazard Analysis (Element Interface Analysis Report)
g Tele-Operator Maneuvering System	Identify critical functions and/or hazardous activities associated with the TMS in concert with the Space Station	Mission Hazard Analysis (Update)
	Apply requirements of NHB XXX and NHB XXY to all TMS/Space Station interfaces	Interface Hazard Analysis (Element Interface Analysis Report)
User (All)	Develop Space Station safety requirements that are station, not mission peculiar	NHB XXY "Space Station Safety Requirements For Operations and Maintenance (Draft)
User (Experimenter)	Identify critical functions and/or hazardous activities associated with the U-E in concert with the Space Station	Mission Hazard Analysis (Update)
	Apply requirements of NHB XXX and NHB XXY to all U-E/Space Station interfaces	Interface Hazard Analysis (Element Interface Analysis Report)
User (Production)	Identify critical functions and/or hazardous activities associated with the U-P in concert with the Space Station	Mission Hazard Analysis (Update)

User (Surveillance)	<p>Apply requirements of NHB XXX and NHB XXY to all U-P/Space Station interfaces</p> <p>Identify critical functions and/or hazardous activities associated with the U-S in concert with the Space Station</p>	<p>Interface Hazard Analysis (Element Interface Analysis Report)</p> <p>Mission Hazard Analysis (Update)</p>
Second Station	<p>Apply requirements of NHB XXX and NHB XXY to all U-S/Space Station interfaces</p> <p>Identify critical functions and/or hazardous activities associated with Space Station-to-Space Station operations</p> <p>Apply requirements of NHB XXX and NHB XXY to all Space Station-to-Space Station interfaces</p> <p>Identify critical functions and/or hazardous activities associated with each interfacing entity</p>	<p>Interface Hazard Analysis (Element Interface Analysis Report)</p> <p>Mission Hazard Analysis (Update)</p> <p>Interface Hazard Analysis (Element Interface Analysis Report)</p> <p>Mission Hazard Analysis (Update)</p>
	<p>Apply requirements of NHB XXX and NHB XXY to all interfaces of each entity</p>	<p>Interface Hazard Analyses per Interfacing Element (Element Interface Analysis Report)</p>

3. SYSTEM ELEMENT DEFINITION INTEGRATION

Common Module Structure	<p>Identify critical function and/or hazardous activities associated with System Element and its operation</p> <p>Initial hazard analysis</p>	<p>Mission Hazard Analysis (Update)</p> <p>Preliminary Hazard Analysis (Update)</p>
	<p>List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue</p>	<p>Element Interface Analysis</p>

Multi-Berthing Adapter

Identify critical function and/or hazardous activities associated with System Element and its operation

Mission Hazard Analysis (Update)

Initial hazard analysis

Preliminary Hazard Analysis (Update)

List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue

Element Interface Analysis

Logistics Module

Identify critical function and/or hazardous activities associated with System Element and its operation

Mission Hazard Analysis (Update)

Initial hazard analysis

Preliminary Hazard Analysis (Update)

List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue

Element Interface Analysis

Resource/Power Module

Identify critical function and/or hazardous activities associated with System Element and its operation

Mission Hazard Analysis (Update)

Initial hazard analysis

Preliminary Hazard Analysis (Update)

List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue

Element Interface Analysis

Laboratory Module	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis
Safe Haven	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis
Contamination/Decontamination Volume(s)	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Apply requirements of NHBYYY to equipment/ functions relating to contamination/ decontamination issues	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis

Remote Manipulator System	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis
Special Use Accessories/Tools	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis
Special Use Accessories/Tools	Identify critical function and/or hazardous activities associated with System Element and its operation	Mission Hazard Analysis (Update)
	Initial hazard analysis	Preliminary Hazard Analysis (Update)
	List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue	Element Interface Analysis

Other Vehicles

Identify critical function and/or hazardous activities associated with System Element and its operation

Mission Hazard Analysis (Update)

Initial hazard analysis

Preliminary Hazard Analysis (Update)

List all inter-element interfaces, identifying critical functions and/or hazardous activities whose bleeding across an interface would be a safety issue

Element Interface Analysis

4. STATION DEVELOPMENT INTEGRATION

System Requirements Review

Ensure Safety Criteria are implemented in requirements documentation

Safety Requirements Matrix

Preliminary Design Review

Conduct preliminary hazard analysis

Preliminary Hazard Analysis Report

Assess program tasks for safety criticality

Safety Critical Procedures Matrix Appendix

Review systems documentation for safety buy-off

Safety Engineering Assessment Log (Entry)

Critical Design Review

Conduct detailed hazard analysis

Safety Analysis Report

Prepare preliminary procedures for safety critical task

Safety Critical Procedures

Define safety verification requirements

Safety Verification Matrix

Review system documentation for safety buy-off

Safety Engineering Assessment Log (Entry)

Prepare risk acceptance matrix

Risk Acceptance Matrix

Critical Design Review (Cont'd.)

First Article Configuration Inspection	Update hazard analysis	Safety Analyses Report (Update)
Design Certification Review	Finalize procedures for critical task Prepare safety certification documentation	Safety Critical Procedure (Update) Safety Certification Report
DD 250 Buy-Off	Review safety data package	Safety Analysis Report (Final)
Launch Preparation Delivery to Orbit Outfitting and Assembly Station/Systems Checkout Station User Systems Checkout Station User Phase-In Full Operations	TBD	

5. LAUNCH COMPLEX DEVELOPMENT INTEGRATION

8

System Requirements Review	Ensure Safety Criteria are implemented in requirements documentation	Safety Requirements Matrix
Preliminary Design Review	Conduct preliminary hazard analysis Assess program tasks for safety criticality Review systems documentation for safety buy-off	Preliminary Hazard Analysis Report Safety Critical Procedures Matrix Appendix Safety Engineering Assessment Log (Entry)
Critical Design Review	Conduct detailed hazard analysis Prepare preliminary procedures for safety critical task Define safety verification requirements	Safety Analysis Report Safety Critical Procedures Safety Verification Matrix

Critical Design Review (Cont'd.)

	Review system documentation for safety buy-off	Safety Engineering Assessment Log (Entry)
	Prepare risk acceptance matrix	Risk Acceptance Matrix
First Article Configuration Inspection	Update hazard analysis	Safety Analyses Report (Update)
Design Certification Review	Finalize procedures for critical task	Safety Critical Procedure (Update)
	Prepare safety certification documentation	Safety Certification Report
DD 250 Buy-Off	Review safety data package	Safety Analysis Report (Final)
Pre-Launch Operations Launch Operations Turnaround Operations Monitoring and Control	TBD	

6. GROUND/AIR SUPPORT LINK DEVELOPMENT INTEGRATION

System Requirements Review	Ensure Safety Criteria are implemented in requirements documentation	Safety Requirements Matrix
Preliminary Design Review	Conduct preliminary hazard analysis	Preliminary Hazard Analysis Report
	Assess program tasks for safety criticality	Safety Critical Procedures Matrix Appendix
	Review systems documentation for safety buy-off	Safety Engineering Assessment Log (Entry)
Critical Design Review	Conduct detailed hazard analysis	Safety Analysis Report
	Prepare preliminary procedures for safety critical task	Safety Critical Procedures

Critical Design Review (Cont'd.)

	Define safety verification requirements	Safety Verification Matrix
	Review system documentation for safety buy-off	Safety Engineering Assessment Log (Entry)
	Prepare risk acceptance matrix	Risk Acceptance Matrix
First Article Configuration Inspection	Update hazard analysis	Safety Analyses Report (Update)
Design Certification Review	Finalize procedures for critical task	Safety Critical Procedure (Update)
	Prepare safety certification documentation	Safety Certification Report
DD 250 Buy-Off	Review safety data package	Safety Analysis Report (Final)
Command and Control Monitoring Data Assessment/Processing Station Operations Phase-In Station Maintenance Phase-In User Operations Phase-In	TBD	

7. LOGISTICS OPERATIONS DEVELOPMENT INTEGRATION

System Requirements Review
System/Subsystem Reliability Assessment
System/Subsystem Maintainability Assessment
System/Subsystem MTBF Definition
Spares Requirement Development
Consumables Requirement Definition
Maintenance Equipment/Tools Requirements Definition TBD
GSE Requirements Definition
Training Requirements Definition
Training Equipment Requirements Definition
Life Cycle Costing
Material Inventory/Control System Development
STS Scheduling/Scheduling Requirements

8. SPACE STATION BUILD-UP OPERATIONS

Module(s) on Dock @ KSC
Module Launch Preparation
Module Launch to Orbit
Interim Airlock Assembly
Module Assembly
Outfitting
Station Personal Equipment Assessment TBD
Station Systems Checkout
Station Accessories/Tools Checkout
Station Operations Checkout
Station Maintenance Checkout
Station/EVA Checkout
Station Operational Shakedown/Full-up

9. ON-ORBIT OPERATIONS (STATION) TBD

10. ON-ORBIT MAINTENANCE (STATION) TBD

11. ON-ORBIT OPERATIONS (USERS) TBD

12. STATION EFFECTIVENESS ASSESSMENT TBD

13. STATION UPGRADING/REFURBISHMENT TBD

14. STATION RETIREMENTS/DISSOLUTION TBD

This Page Intentionally Left Blank

Appendix BA
APPLICABLE DOCUMENTS

SPACE STATION SAFETY APPLICABLE DOCUMENTS

NHB XXX	"Safety Requirements for Space Station Users, Experimenters and Interfacing Vehicles and Hardware"
NHB XXY	"Space Station Industrial Safety and Health Requirements"
JSC 1000 (TBD)	Safety, Reliability, Maintainability and Quality Provisions for the Space Station Program
NHB 1700.7A	Safety Policy and Requirements for Payloads Using the STS
KHB1700.7A/ SAMTO HB S-100	Space Transportation System - Payload Ground Safety Handbook

This Page Intentionally Left Blank

PRELIMINARY SPACE STATION CREW SAFETY THREAT LIST

The threats listed here are generic in that each threat may have more than one possible cause. Further in this study, potential hazards will be developed for these threats, allowing specific identification of controlling safety criteria and guidelines.

The scope of issues covered are threats that affect crew health and well being directly and threats that impact the space station and its ability to continue functioning. Sources of threats can be external to the space station, crew initiated, space station hardware/software responsible, or generated by hardware/software and processes dedicated to space station experiments, payloads, and cargo.

Design and operational guidelines eventually will have to be drawn up for the space station and its dedicated crew equipment, for crew functions, as well as for carry-ons: experiments, payloads and cargo.

FIRE

A fire in an area containing subsystems equipment, electrical wiring, or laboratory equipment, or in personnel areas which damages and puts out of commission all unprotected operating equipment in a compartment. Fire prevention in design leans heavily on isolating the elements of combustion: Fuel, Oxidizer and Ignition. In a two-gas system (80% N₂ and 20% O₂) the fuel is excluded only if all materials are screened for flammability. Applying "NASA MSC Requirements for Materials and Processes", JSC-SE-0006B, through the RI-SD Material Control (MATCO) program screened shuttle materials for flammability. In a 100% O₂ environment (such as in EVA pre-breathing areas), all surface temperatures must be analyzed to ensure that no ignition sources are available and the contained materials are not flammable at high O₂ concentrations. "Environment Requirements and Test Criteria for the Orbiter Vehicle", MF0004-014C, cites maximum allowable surface temperatures in each of the compartments based on the potential fluid leaked into the compartment. Fluid leaks are considered credible. Additionally, smoke/fire sensing and suppression could be included in Damage Control design.

LEAKAGE

Leakage of any gas or liquid which is produced, stored, or routed through the pressurized areas of Space Station volumes, including any chemicals used or that may be produced in experiments. The leakage may occur at any point through which the fluid is routed. Leakage rates must be assumed and increased margins and/or system make-up capability must be included in the design. Selection of materials and seals for faying surfaces is critical to the life of the Space Station in orbit. Seal selection, expected life, condition at installation, and installation techniques determine leak susceptibility at all penetrations.

TUMBLING/LOSS OF CONTROL

Space Station attitude maintenance systems require at least fail-operational/fail safe capability. Consideration of a requirement for maintenance and returning the system to operable status should be given. Forces that may cause tumbling or loss of control, other than attitude

maintenance system failure, could include: moments imparted by Orbiter/OTV docking or collision, fluid or gaseous systems leaking/venting, crew activity within the station, and the like. Recovery from and immediate reaction to Space Station tumbling should be a system design requirement including center of gravity and mass distribution effects.

BIOLOGICAL OR TOXIC CONTAMINATION

Contamination threats are those associated with biological or toxic contamination of the food or water supply. All similarly packaged food stored in any one area (e.g., all vacuum-packed food stored in one pantry) will be assumed unfit to eat. Similarly, all potable water in connected tanks will also be assumed toxic; the water, however, may be reprocessed through the water purification system and the tanks decontaminated to render water potable. This threat is associated with the release of toxic, flammable, corrosive, condensible, or particulate matter. Contamination is caused by leakage, spillage, outgassing, loose objects, abrasion and from the growth of fungus or release of volatile condensible materials. Leakage of or outgassing of hazardous materials should be prevented by eliminating suspect materials through MATCO screening. Close looks at materials interactions are also required. Where hazardous materials are brought on board, special containment consideration must be given. All materials brought on board should be screened, including astronaut personal effects.

INJURY/ILLNESS

Physical injuries may be caused by impact or collision with stationary objects having sharp edges or protruding parts or with shrapnel or projectiles from exploding tanks or accelerated loose objects. Physical injuries may also be caused by ingesting particulate matter, touching hot or cold surfaces, and by breathing oxygen deficient air. Care and control to prevent sharp and abrading protrusions and the inclusion of hand holds and other convenient restraints for astronauts minimizes exposure to injury. Crew illness could result from exposure to pathogenic bacteria, toxic materials, or to excessive radiation levels. The physiological/behavioral impact of microgravity of the crew for long time exposure is not clearly understood. Personal hygiene and close control of food preparation minimizes exposure to illness. Crew illness and injury must be treatable within the Space Station. The sophistication of medical facilities is yet to be determined. Death of an astronaut cannot be ruled out, raising the question of what procedure is to be followed for the disposition of the remains, i.e., return to earth or burial in space - burial at sea precedence.

GRAZING/COLLISION

This threat concerns internal as well as external elements and can be caused by structural failure, procedural error or inadequate stowage and handling rationale. External threats can be caused by Orbiter/OTV or EVA astronauts coming into unplanned contact with the Space Station. A grazing collision with another vehicle which damages equipment outside the spacecraft, such as RCS jets, radiators, solar panels, antennas, tanks, fluid lines, docking mechanisms, etc., is considered here. The collision is not severe enough to cause a penetration of primary structure but may damage exposed equipment. Potential collision candidates must be identified and the specific threat defined.

CORROSION

This threat concerns structural degradation of metallic and nonmetallic equipment. Leakage of corrosive or reactive materials can degrade an equipment's usefulness. Material incompatibility at joints of dissimilar metals can lead to corrosion when subjected to internal environment extremes of temperature and humidity accelerating corrosion in carbon or most organic materials. Examples of corrosive processes include stress corrosion, electrolytic corrosion, and polymerization. Causative agents include acid, salts, solvents, halogens, etc. The MATCON program is set up to screen against corrosive agents and processes.

MECHANICAL DAMAGE

Mechanical damage is defined as being caused by collision inside the vehicle with loose out-of-control masses. Damage potential of systems requires assessment as to impact on mission continuation, type of emergency precipitated, postulated damage, protection affordable in design and mission recovery impact. External causes (Fire, Explosion, Collision, Penetrations, Attack, Sabotage or Human Error) may not be preventable, requires that system damage tolerance should be a significant design consideration for critical systems.

EXPLOSION

In the event of an explosion, the damage will be confined to one compartment and will consist of overpressure, heat, shrapnel, and atmospheric contaminants. All equipment in the compartment may be damaged and made inoperative, unless armor-plated for protection. Violent release of energy as a result of equipment overpressurization, fire, chemical reaction, excessive temperature, equipment malfunction or structural failure are candidate causes for explosion. For instance, an explosion of .025 lb TNT equivalent, releasing 50 BTU of energy in the form of heat, shock waves and kinetic and thermal energy of shrapnel damage could be confined to one compartment and would consist of overpressure, heat, shrapnel and atmospheric contaminants. The equipment would require repair/replacement, depending on the damage an explosion can produce. Further hazards which can result in a compartment by such an explosion, such as fire, etc., should also be considered as part of the threat. Walls and primary structure, or equipment outside the affected compartment, would probably not be damaged. (021) Equipment which can disintegrate explosively includes pumps, motors, blowers, rocket motors, generators, laser, etc. In excluding equipment and materials from Space Station habitable volumes whose TNT equivalency exceeds TBD, explosion impact can be minimized. Equipment and material mounted externally to the Space Station habitable volumes that exceed the threshold TBD TNT equivalency should include shrapnel diverter shields to protect the habitable volumes from catastrophic penetrations. Guidelines concerning pressure sensing, relieving and control, chemical screening to prevent use of violent reagents, and system heat rejection are key elements controlling explosion risks.

LOSS OF PRESSURIZATION

A loss of pressurization in a habitable volume may be caused by an accidental penetration of an outside wall or bulkhead. Pressure sensing, leakage and maintenance imply the need for a Damage Control System on-board the Space Station. Such a system would include pressure, temperature and toxicity sensing with additional capability for smoke sensing and fire

suppression for each isolatable compartment in the Space Station with primary and back-up readout panels located in separate Space Station areas. If compartment size and criticality so indicate, a need may exist for automatic control of hatch actuation. These design constraints are dependent upon assumed penetration size, size of each isolatable volume, use frequency of the compartment and criticality of the adjacent compartments.

RADIATION

Radiation threats are associated with the exposure of the astronauts as well as equipment to ionizing radiation, ultraviolet or infrared light, lasers, and electromagnetic or radio frequency radiation. Ionizing radiation threats may be caused by leaking or inadequately shielded radioactive equipment such as RTG's, particle accelerators, liquid metal heat exchangers, etc. RF and electromagnetic radiation from RF generators can trigger ordnance devices or interfere with the operation of critical equipment. Allowable levels of each of these energies must be established, and design accommodation made to ensure that the Space Station astronauts and equipment are protected.

OUT OF CONTROL IVA/EVA ASTRONAUT

Loss of control of astronauts during IVA/EVA may be caused by malfunctioning maneuvering devices or lack of adequate handholds and other restraints. The issue of aberrant astronaut actions causing a problem must be considered. Rapid rescue is required by a companion already suited and conditioned to the suit atmosphere, who is waiting in an airlock or is also performing EVA or IVA. Equipment adequacy and redundancy could address the former issue, the latter may require some physical restraint system, equipment or facility.

INADVERTENT OPERATIONS

Critical tasks and systems controls should be analyzed to assess the impact of inadvertent operations. Hardware can be protected by switch wickets, lever-locks, etc. Software can be protected by two or three "and"-ing requirements, as well as being protected from astronaut modification on-board. Recommendations are for automating all routine functions, with manual work-arounds as required.

LACK OF CREW COORDINATION

Within the aviation industry - both civilian and military - experience has shown that lack of crew coordination in times of crisis has almost invariably resulted in catastrophe. Some of the recent major disasters in commercial air travel have occurred as a result of the entire crews' attention being diverted to trouble shooting the problem affecting the airplane while no one paid attention to the ordinary chores of piloting and navigating the airplane. One major airline radically changed crew training and upgrading techniques to address this problem. Similar problems of lack of crew coordination could arise in a Space Station. It is important that critical routine functions be manned at all times, if not automated. This will allow investigation of malfunctioning equipment by personnel not dedicated to routine, but essential, Space Station equipment. Crew tasks should be reviewed carefully with this potential problem in mind.

ABANDONMENT OF SPACE STATION

There should be a passive capability of the Space Station to survive abandonment. A combination of accidents and/or subsystems degradation requiring the abandonment of the station by some or all of the occupying personnel is considered here. Such abandonment will not be a time-critical emergency but a deliberate abandonment planned over a period of days to months. The worst design case is when one of the separate pressure volumes has been evacuated and sealed off for some time because of major damage or contamination, and all personnel are in the remaining volume. If the cause for abandonment concerns the inability of the station to support human habitation, the station should be able to maintain critical functions, such as attitude maintenance. A cause for abandonment could be loss of a breathable atmosphere. Critical avionic equipment should be able to function in the absence of an atmosphere. An important task related to the above hazard, that was considered during this effort was the Escape and Rescue. The philosophy adopted with respect to escape and rescue is stated below:

Increased Reliability or Redundancy	Preventive		Built-In
Damage Control Compartmentalization	Preventive		Built-In
Improved Emergency Sensors	Preventive		Built-In
On-Board Preventive Maintenance	Preventive		Built-In
Abort Capability	Remedial		Built-In
Personal Survival Equipment	Remedial	Separate	Built-In
On-Board Repair Capability	Remedial	Separate	Built-In
On-Board Medical Aid	Remedial	Separate	Built-In
On-Board Emergency "RED" Systems	Remedial	Separate	Built-In
"Buddy" Concept (Separate Type)	Remedial	Separate	
On-Board Escape and Wait	Remedial	Separate	
On-Board Escape and Return	Remedial	Separate	
Spare Earth Return Module	Remedial	Separate	
Unmanned/Manned Assistance or Rescue			
Earth Launched (Post Emergency)	Remedial	Separate	
"Pre-Deployed"	Remedial	Separate	

ELECTRICAL SHOCK

When personnel, during the normal operations of equipment or due to single point failures or masked dual point failures, are exposed to electrically energized components, terminal strips, buss bars, stored charge apparatus, etc., that through a combination of electrical potential, current and body resistance would allow a person's body to offer a path for current flow to ground and result in shock or electrocution, a hazard potential exists. A hazardous voltage or power source is any potential source of power that can produce serious shock or burns or a fatal current, dependent upon body resistance, contact conditions, and path through the body (see table below). Also equipment which senses or controls critical control parameters of flight systems or is reasonably capable of applying damaging electrical energy to supported systems is classified as Safety Critical.

PROBABLE EFFECTS OF SHOCK

Current Values (Milliamps)

AC 60HZ	DC	Effects
0-1	0-4	Perception
1-4	4-15	Surprise
4-21*	15-80*	Reflex Action
21-40*	80-160*	Muscular Inhibition
40-100*	160-300*	Respiratory Block
Over 100*	Over 300*	Usually Fatal

*Serious Shock or Burns.

METEOROID PENETRATION

A fallout of space debris studies will have to be a probability of strike and an assumed size of meteoroid. The potential impact of this threat has not been specifically defined at this time. However, basic assumptions should consider potential meteoroid penetration of the primary structure. Physical damage should be confined to one compartment and is assumed to consist of finely divided molten high-speed shrapnel (from spallation of the inner wall).

STORES/CONSUMABLES DEPLETION

Consumables, both for the Space Station as well as for the astronauts, require establishing levels that account for leakage, spoilage, unexpected high consumption rates, etc. The key to establishing quantities, is determining what survival time, without support from the ground is required: 96 hours, seven days, or what? Automatic inventorying of critical consumables should be considered.

INTRUSION/ATTACK

Screening related literature indicates that intra-crew member hostility was an issue on the longer space flights. When space stations evolve and less highly motivated and dedicated personnel are included in crews, special screening of candidates will be required. This threat could be psychological

as well as physical. STS-5, and subsequent flights where more than two crew members are on board, will be watched closely as crew interaction will be more complex. How to approach the impact of this threat: with sedation, by employing "Polaris Pajamas", by isolating offending crew members, etc. - must be determined. Overt military action and external intrusion/attack is a fallout of a space station survivability analysis and is beyond the scope of this study.

STRUCTURAL EROSION

This issue has been observed in long lived spacecraft. Space debris and other minutia progressively can erode metallic or non-metallic enclosures to the point where leakage could occur. If the eroded skins allow fluid or gas containment systems to leak, undesirable spin/tumbling moments could be reacted into the space station and/or consumables could be lost overboard. This is a downstream "wear" issue but appears to be real enough to address in the program.

ORBIT DECAY

Consumables needed to update orbital position or to overcome the effects of space station drag may become an issue when large captive structures are being constructed prior to separation from the space station. Credibility of this threat is understood when one considers a fully operational space station in its planned working environment. This threat impacts consumable margins.

LOSS OF ACCESS TO A HATCH

The loss of access to any one hatch, door, or other personnel or cargo transfer opening because of jamming of the mechanism, either open or closed; or because of obstruction by cargo; or because of a localized hazardous situation (fire, chemical spillage, electrical hazard, etc.). Compartmentation to allow access to "safe havens" requires a minimum of two egress paths from each habitable volume. Present space station design philosophy appears to provide this capability. Design drivers are hazards that destroy compartment habitability and require survival workarounds.

TEMPERATURE EXTREMES

Ability of crew and equipment to function under varying temperature stresses needs to be considered. Emergencies such as the Apollo 13 Service Module tank explosion, may be postulated to determine the credibility of this threat. Unexpected heat inputs from experiments/payloads/cargo need be addressed early to ensure the space station's ability to grow into its operational phase. This threat deals indirectly with planned EC margins and absolute capabilities.

DEBRIS

The threat category of external debris includes objects in excess of meteoroids in size, usually referred to as space garbage. Nominally, space debris, as opposed to meteoroids, would have lower closure rates allowing the possible option of collision avoidance. Internal debris, on the other hand, can clog filters and directly affect equipment operation and crew performance. The Orbiter has experienced clogged filters due to lint, affecting air cooled avionics and overloading fan motors.

This Page Intentionally Left Blank

Appendix BC
SPACE STATION
CREW SAFETY CRITERIA

These criteria were eclectically assembled from industry space station studies beginning as early as 1968. Those criteria that were relevant to the current space station studies were carried forward, if not in detail, at least in intent. Reassessment of threats under Contract NAS1-17242 evolved additional criteria that are included.

20 January 1984
Rockwell International
Space Transportation and
Systems Group

DAMAGE TOLERANCE

- A-1 No credible single space station failure, operational error or radio frequency signal should result in damage to space station or mission/payload equipment or in the use of emergency equipment; some limited degradation in mission/payload accommodations, crew convenience/comfort, or space station attitude or orbit may be allowed
- A-2 No credible combination of two space station failures, mission/payload equipment failures, operator errors, or radio frequency signals should result in the potential for crew injury or permanent loss of the space station or primary mission/payload capability; institution of emergency procedure/equipment may be necessary but no hazardous operational level will be reached
- A-3 All subsystem/equipment critical to preservation of life and space station survival shall be fail-operational/fail-safe (excepting primary structure and pressure vessels)
- A-4 Fail-operational/fail-safe designed subsystems should allow maintenance to upgrade the subsystem/equipment without being degraded below fail-safe during the maintenance actions following the second failure
- A-5 Potentially rupturable containers should contain less material (gas, liquid, solid) than would cause unacceptable overpressure if all the material were released in a leakage, rupture or explosion
- A-6 Redundant accommodations for command and control of the space station shall be provided such that the primary control center has complete capability, but the backup control center will have, as a minimum, control of critical functions
- A-7 Design inhibits to prevent failure propagation from one volume/subsystem/component to another should be incorporated
- A-8 The space station should be designed and operated so that any damaged module can be isolated from the rest of the Station in TBD seconds, as required. Provisions shall be made for pressure isolation within the volumes. Modules should be equipped and provisioned so that the crew can safely continue a degraded mission and take corrective action to either repair or replace the damaged module
- A-9 Any volume should be capable of sustaining the whole crew, and capability should be provided for performing critical functions at an emergency level until the crew can be rescued. Electrical and fluid lines in each pressure-isolatable volume required for critical functions should be protected against the effects of explosion, fire, vacuum, and corrosion

- A-10 Capability should be provided for performing critical functions with a portion of a subsystem inoperative for maintenance, and any pressure-isolatable volume inactivated and not accessible
- A-11 Redundant equipment, lines, cables, and utility runs which are critical for safety of personnel or mission continuation should either be located and routed in separate compartments (i.e., separated by a structural wall) or should be protected against fire, smoke, contamination, loss of pressure, overpressure, and shrapnel
- A-12 All walls, bulkheads, hatches and seals whose integrity is required to maintain pressurization or atmospheric isolation shall be readily accessible for inspection and repair by crewmen in pressurized suits
- A-13 As a design goal, inspection, maintenance and repair of critical subsystems by shirt-sleeved crewmembers shall be accommodated.

CREW PROTECTION

- B-1 Provisions should be made for a safe haven within the space station, isolatable from the hazard capable of sustaining the crew for 21 days beyond normal resupply and allowing rescue by a Shuttle. Provisions shall be made to monitor the health of the remaining habitable modules from this safe haven
- B-2 Personnel protection from electrical shock, radiation, mechanical and thermal hazards should be provided
- B-3 Accessways between compartments should be sized such that an IVA/EVA-suited crewman is allowed free passage
- B-4 Provisions shall be made for the protection and survival of the whole crew during solar storm activity as defined by the TBD design mission radiation model
- B-5 Personnel escape routes should be provided in all hazardous situations
- B-6 Provisions and habitable facilities should be adequate to sustain the entire crew for a minimum of 22 days during an emergency situation when damage repair is in progress
- B-7 Atmospheric stores and subsystem capability sufficient for two full repressurizations of each pressurized habitable volume should be maintained on/at the space station during manned operations
- B-8 Access to EVA and IVA airlock and suit station(s) should be provided for all credible emergency conditions. Airlock chamber(s) should be provided to permit crew access for EVA/IVA operations
- B-9 Two or more suited crewmen should participate in any pressure suit activity and rescue provisions should be provided to allow safe return to space station, following the incapacitation of any one crewman
- B-10 Real-time monitoring of the atmosphere constituents, including harmful airborne trace contaminants and odors should be performed. Control shall be provided for each pressurized habitable volume

- B-11 Two or more entry/egress paths should be provided to and from every module or pressure-isolatable volume. The two paths should be separated by airtight partitions, or shall be at least 10 feet apart, and should each lead to an area in which the crew can survive until escape, rescue or removal of the hazard
- B-12 Materials used in the habitable areas should not outgas toxic constituents in the lowest pressure environment and highest temperature to which they will be exposed
- B-13 All EVA and unpressurized compartment IVA should be conducted using the "buddy system". (Note: buddy system criteria can be met with suited crew to station exit in visual contact with subject.) The buddy system should also be used during shirtsleeve operations in hazardous areas
- B-14 A margin of consumables should be provided onboard, sufficient for performing critical functions for TBD hours at a reduced level following any credible accident which renders one pressure-isolatable compartment unavailable
- B-15 At least two egress paths should be available from each module for emergency egress of personnel during manned ground operations
- B-16 Emergency pressure suits required in the space station, sized to fit any crewman, should be in readily accessible locations within each pressure-isolatable volume
- B-17 Provisions should be made for emergency medical treatment of credible accidents and illnesses for durations compatible with the rescue provisions
- B-18 The safe environment and the safe operational status of activated subsystems within the space station should be verified prior to personnel entry, initially and prior to reentry following temporary station abandonment
- B-19 Deployment and initiation of operations considered hazardous should be checked out from a safe location before exposing crewmen to the potential hazards
- B-20 Provision should be made for the return of a crewman incapacitated while performing EVA
- B-21 Provisions should be made for the detection, handling, containment and/or disposal of toxic, flammable, combustible and hazardous materials
- B-22 Pressurized volumes should have adequate free volume (not occupied by equipment) to allow crew freedom of movement to support long-duration habitation
- B-23 Hazardous or toxic fluid storage, conduits and interconnects between modules should be external to the pressurized volume. Exceptions may be made for flammable but nontoxic gases where the maximum possible quantity released by a leak cannot result in a flammable mixture

- B-24 Provisions should be made for detection and control of pathogenic agents onboard the space station using methods harmless to crew and equipment
- B-25 Planned crew tasks should be assessed initially, for compliance intent with TBD regulations before performing such tasks; and crew training provided for each specialized and/or hazardous task
- B-26 Provision should be made for handling irrational crewmembers and the remains of deceased crewmembers
- B-27 The occupied compartment's acoustical noise environment should be within human tolerance noise exposure limitations, permit intelligible auditory communications, have a minimum of pure tone or narrow frequency band(s), a minimum of intermittent or discontinuous noises and a minimum of high-frequency noises. System and equipment design (including subcontractors) should be accomplished from the outset to produce an acceptable noise environment. Desirably, the noise environment should meet NC TBD-or-lower noise contour for work periods and NC TBD-or-lower for sleep periods
- B-28 Any module designated as a safe haven shall be provided with an airlock chamber at the port assigned for orbiter docking and rescue, to allow crew transfer and rescue from a degraded and/or marginal safe haven. The rescue hatch shall provide for actuation from inside or outside to accommodate contingencies
- B-29 Subsystems shall be designed to prevent inadvertent or accidental activation or deactivation of functions or equipment that would be hazardous to personnel or the Space Station
- B-30 Radiation doses that affect personnel safety must be considered from all sources, including natural environment, external isotope and reactor sources (if any), electromagnetic, solar radiation and internally allowable radiation levels from experiments, processes and health maintenance/diagnostic equipment
- B-31 Exposed surfaces within habitable modules shall not exceed a temperature of 113°F (with a design goal of 105°F) and a low temperature of no less than 40°F
- B-32 Except for contingencies EVA shall not be used for hazardous operations or when a maneuvering spacecraft is within the proximity operating zone (+5 nm)

STATION INTEGRITY

- C-1 Primary pressure structural materials should be nonflammable. Interior walls and secondary structure should be self-extinguishing
- C-2 Normally exposed nonmetallic materials should be self-extinguishing in the most severe oxidizing environment to which they will be exposed. Means shall be provided for fireproof storage of medical supplies, maintenance supplies, food, tissue, clothing, trash, and for other non-self-extinguishing items, when they are not in use

- C-3 Potentially explosive containers such as high pressure vessels or volatile gas storage containers shall be placed outside of and as remotely as possible from personnel living and operating quarters. Wherever possible the containers should be isolated and protected so that failure of one will not propagate to others
- C-4 Containment of all materials requiring return via the STS to prevent contamination of the space station environment should be provided to reduce the hazard of potential fire and toxic conditions
- C-5 Tank supports should be designed to restrain the tank under propulsive effect of rapidly escaping gas
- C-6 Design provisions should be incorporated to prevent uncontrollable hatch opening due to pressure differentials, and to allow controlled closing of hatch openings with or against pressure differentials, for the worst case pressure differentials anticipated
- C-7 Equipment or materials sensitive to contamination should be handled in a controlled environment. Fluids and materials should be compatible with the combined environment in which they are employed
- C-8 Provisions should be made to allow communication between any and all isolatable/habitable volumes on a primary and backup basis
- C-9 Provisions should be made for material usage, identification and location mapping to allow real-time evaluation to determine adequate inspection/maintenance replacement frequencies
- C-10 Fluid or gaseous flow such as pressure relief valves/exhausts, fuel transfer disconnects, etc., should be designed to prevent torquing/turning or undesirable translation motions to the space station
- C-11 All reaction control thrusting devices used primarily for altitude positioning of the space station, and occasionally for velocity changes, should be located such that the exhaust plume does not impinge upon other structural elements such as solar cells, areas requiring EVA maintenance or other vehicles docking with the space station
- C-12 Space station modules should be tumbled to rid them of internal debris and contaminants immediately prior to preparation for launch
- C-13 Provisions shall be made for in-flight servicing, adjusting, cleaning, removal and replacement of offending components, testing and repairing of all critical subsystems
- C-14 Wear items should be life cycle tested in a realistic environment
- C-15 All personal items should be screened for flammability and toxicity

- C-16 Space Station protective enclosures shall be provided for all high mass/high speed rotating machinery
- C-17 Active/passive compartmentation should be provided to contain and/or prevent fire/explosion/depressurization initiation or impact propagation. Compartments should be inspectable to support damage control and maintenance operations.

CONTINGENCY CONTROL

- D-1 Identified hazards should be eliminated, reduced to controlled hazards, or specified as residual hazards
- D-2 Provision should be made for detecting, annunciating, containing/confirming, controlling and restoring to a safe condition emergencies such as fire, toxic contamination, depressurization, structural damage, etc. The tools, tasks, spares, workspace, storage volumes necessary for these provisions shall be included in space station design planning
- D-3 For those malfunctions and/or hazards which may result in time-critical emergencies, provision should be made for the automatic switching to a safe mode of operation and for caution and warning of personnel
- D-4 The capability should be provided on the space station for the detection of malfunctions and/or hazards, tracing to the failed replaceable unit and the display of information to the crew necessary for corrective action
- D-5 Provisions should be made for the crew to ascertain the hazard status of any habitable module external to the inhabited module and to mitigate or control remotely those hazards which would preclude safe entry to the module in question
- D-6 The crew must be able to override any automatic safing or switchover capability. All overrides should be two-step operations with positive feedback to the initiator, which report impending results of the override command, prior to the acceptance of an execute command
- D-7 Windows should be provided in the space station to enable adequate visibility to accomplish safe docking operations with the orbiter or other vehicles. Additional windows will be necessary to monitor EVA operations, logistic resupply operations and to support photographic requirements. Transmission through the windows should be such as to protect the crew from harmful UV and IR radiation. Thermal flux from the windows should be controlled to prevent excessive heat from the crewman's face and head
- D-8 An independent self-contained illumination system should be provided that will be automatically activated in the event of a major primary power failure or main lighting circuit malfunction resulting in circuit breaker interruption
- D-9 Materials and components subject to insidious degradation in the Space Station ionizing radiation environment shall not be used where that degradation can cause or contribute to a crew hazard

D-10 Provisions shall be made for safe disposal of the Space Station or any auxiliary part thereof without danger to flight or ground crew-members or the public

SELECTION/INDOCTRINATION

- E-1 Crew selection should be based on selectees cross-trainability in fields other than speciality
- E-2 Orbital crews should be an integral part of the air/ground system active interface with on-orbit crews
- E-3 Station crews and teaming should allow equal thirds of schedule for on-orbit, ground interface operation and recycle operations (post orbit rehabilitation, leave, additional training, public relations, etc.)
- E-4 Assurance should be provided that each mission segment crew is familiar with 1) Station Operations and Maintenance as concerns critical subsystem and 2) Procedures necessary to render SAFE all experiments and/or user-processes
- E-5 Screening criteria should include assessment of attitudes, physical needs, psychological needs, personality traits, ability to function under stress, ability to accept direction, and TBD

Appendix BD
SPACE STATION
CREW SAFETY DESIGN GUIDELINES

These design guidelines were eclectically assembled from industry space station studies beginning as early as 1968. Those guidelines that were relevant to the current space station studies were carried forward, if not in detail, at least in intent. Reassessment of threats under Contract NAS1-17242 evolved additional guidelines that are included.

21 February 1984
Rockwell International
Space Transportation and
Systems Group

SPACE STATION SAFETY GUIDELINES

Design Guidelines Acronyms

AOM = Attitude/Orbit Maintenance Systems
C&W = Caution and Warning Systems
CME = Crew Messing Equipment
COM = Communication Equipment
CPH = Cargo/Payload Handling Systems
CSE = Crew Safety Equipment
CWS = Crew Water Systems
DPS = Data Processing Systems
DUS = Docking/Undocking Systems
ECS = Environment Control System
EPD = Electrical Power Distribution Systems
EPG = Electrical Power Generating Equipment
FSE = Fluid System Equipment
HMS = Health Maintenance Systems
IFM = In-Flight Maintenance
INT = Integration, two or more systems involved
MSE = Mechanical Systems Equipment
NUC = Nuclear/Ionizing Radiation Systems Equipment
OPS = Operations
RSD = Radiation Shielding Devices
STR = Structural Systems

SPACE STATION CANDIDATE SAFETY DESIGN GUIDELINES

DG-INT-001. Normally habitable compartments of more than 25 cubic meters (880 cubic feet) in volume shall have two or more exits into areas which provide for personnel survival. These exits shall be at least 3 meters (10 feet) apart.

DG-INT-002. Flammable, explosive or gas generating material shall be located so that the energy content which can be propagated at any one location shall not result in overpressurization of the compartment from heat and gas production.

DG-INT-003. Flammable, explosive or gas generating material within 3 meters (10 feet) of the entrance to compartments with only one entry/egress path shall be limited so that the energy content, if released, will not result in damage or an environment which prevents shirtsleeve access through the entrance.

DG-INT-004. Two or more entrances into normally habitable compartments of more than 25 cubic meters (880 cubic feet) in volume shall be shirtsleeve accessible from each of the other normally inhabited compartments. These entrances shall be at least 3 meters (10 feet) apart.

DG-INT-005. Where only one shirtsleeve ingress/egress path is provided into a compartment or module, redundant means shall be available for opening the connecting hatch(es) from either side.

DG-INT-006. Capability shall be provided to depressurize adjacent volumes before undocking.

DG-ECS-007. Capability shall be provided to reduce the pressure in each habitable volume sufficiently, or increase it in the adjoining habitable volumes and to cut off air circulation, so that in an emergency the atmosphere in the affected volume will not be propagated into adjoining compartments. This capability shall be controlled remotely from each compartment.

DG-ECS-008. Automatic venting capability shall be provided in each habitable volume so that in the event of a fire or release of gases within the volume the pressure will not exceed the structural limits of the structure or the capability of the seals to other volumes to exclude the contaminated atmosphere.

DG-INT-009. Double contained toxic flammable or corrosive fluid containers shall be provided, with means to detect leakage of the toxic flammable or corrosive fluid into the volume in between the containers, and with means to detect penetration of the outside container.

DG-INT-010. Capability shall be provided to detect potential tank failures by measurement of fluid pressures, temperatures, tank strains, or other means.

DG-INT-011. The reflectance of surfaces of docking vehicles and the docking system that are visible to the controlling crew and TV cameras shall be below eye and vidicon damage levels.

DG-DUS-012. The vidicon tubes for docking shall be designed for low sensitivity to tube image burn.

DG-DUS-013. Redundant or replaceable lighting provisions shall be provided for docking.

DG-DUS-014. Redundant or replaceable vidicon tubes shall be provided for docking.

DG-DUS-015. Redundant or replaceable video monitors shall be provided.

DG-DUS-016. Docking system rapid emergency release capability shall be provided.

DG-DUS-017. The docking system shall be designed to withstand normal jackknifing vehicle dynamics and will limit attitude excursions to within prescribed limits as determined by space station geometry to prevent inadvertent contact from the docking vehicle.

DG-DUS-018. The docking system shall be capable of withstanding vehicle oscillations and loads generated by inadvertent attitude control system activity of either or both vehicles during draw down to rigidize the capture interface.

DG-INT-019. Thermal protection shall be provided to prevent jet plume impingement damage to the space station from docking vehicles within the design angular and linear misalignments.

DG-IFM-020. Capability shall be provided to recycle both capture and seal latches on the docking system from any phase of their status.

DG-INT-021. All hardware in the docking tunnel will be flush mounted to interior walls of the cargo/crew transfer tunnel.

DG-MSE-022. Stops shall be provided on hatches to prevent uncontrolled opening if opened when a pressure differential exists.

DG-DUS-023. All docking interface equipment shall be grounded.

DG-DUS-024. At the docking ports, all electrical umbilicals shall be grounded until connection of the docking interface.

DG-INT-025. Capability shall be provided for the emergency shirtsleeve survival of all on-board personnel until the next resupply or emergency shuttle flight following the loss of access to any one module/compartments. A shirtsleeve accessible docking port shall be available. If the loss of the habitable volume divides the space station into two or more isolated habitable sections, then each section shall provide the survival capability for all on-board personnel, including an available docking port.

DG-INT-026. A backup EVA egress/ingress hatch which can be used for contingency EVA shall be available. Capability for depressurization and repressurization of the connecting habitable volume shall be provided.

DG-INT-027. An emergency IVA or EVA return route shall be available for any planned IVA activity independent of the normal IVA airlock route. Depressurization and repressurization capability shall be provided for the additional volumes which must be used.

DG-CSE-028. Emergency portable life support systems shall be available in the airlock sufficient to sustain IVA personnel in an emergency IVA or EVA return from planned IVA or EVA activity.

DG-COM-029. Communication between any and all habitable/isolatable volumes on a primary and backup basis shall be provided.

DG-EPG-030. Adequate venting of batteries shall be provided to prevent contamination, overpressure or explosion.

DG-FSE-031. All filters, screens or other devices used to collect contaminants or waste products shall be designed so they can be easily serviced or replaced without releasing contaminants into the atmosphere.

DG-C&W-032. An audible and visual alarm shall be provided to warn the crew of habitable volume CO₂ partial pressure not within the prescribed limits for crew safety. This alarm shall be provided both in the affected habitable volumes and at the command and control center(s).

DG-EPD-033. Equipment, including electrical wiring, that could become contaminated or damaged by leaking propellants shall be located to prevent contact with possible leakage or shall be provided with suitable protection.

DG-INT-034. Means shall be provided for collecting and/or containing any loose fluids or debris that may result during replacement of system components.

DG-FSE-035. Fluid systems shall have provisions for shutting off the flow of fluid to sections of the system or equipment which are susceptible to damage or leakage.

DG-FSE-036. All orifices, close tolerance valves and contamination-sensitive equipment in fluid systems, shall be adequately protected from contamination. Furthermore, if the system is designed for periodic flow reversal, or a possibility exists that flow reversal can occur, both sides of these items shall be protected.

DG-CME-037. Food supplies shall be stored in more than one storage container.

DG-CME-038. A means for sterilizing containers where food is stored shall be provided.

DG-CME-039. Food supplies which require cooling or refrigeration shall be protected by a redundant capability.

DG-HMS-040. Means for controlling insects in the space station shall be provided. The control method should be harmless to men and equipment.

DG-INT-041. The use of mercury on-board space stations should be prohibited.

DG-ECS-042. Provision shall be made for the removal of ozone generated by X-ray equipment or electrical arcs.

DG-FSE-043. The number of connectors used to connect plumbing or components in fluid systems should be kept to a minimum.

DG-FSE-044. Safety requirements for all subsystems/experiments/internal payloads are needed.

DG-FSE-045. Fluids required for operation of subsystems located in habitable volumes shall be non-toxic, non-flammable, and non-corrosive.

DG-INT-046. Pressurized containers should not be installed in normally habitable volumes. When installed externally to normally habitable volumes, shrapnel shields shall be provided to protect the normally habitable volumes.

DG-C&W-047. Visual and audible alarm shall be provided to warn the crew of atmosphere contamination which exceeds the limits established for crew safety. This alarm shall be provided at a minimum in the affected habitable volume and at the command and control center(s).

DG-C&W-048. Where the possibility exists that a fluid in a system could become contaminated, means shall be provided to detect contamination and provide an alarm at the command and control center(s).

DG-C&W-049. A system shall be provided to monitor the environmental status of all potentially hazardous (explosive, flammable, toxic, etc.) materials stored on-board the space station, and display a warning signal in the command and control center(s) when established limits are exceeded.

DG-C&W-050. A warning and alarm system shall be provided to alert the crew of atmosphere relative humidity levels which are not within prescribed limits, with the warning displayed at the command and control center(s).

DG-ECS-051. Provisions shall be made for containing, venting or eliminating odors and bacteria generated by waste products and other sources.

DG-ECS-052. The composition of the space station water supply shall be checked at regular intervals to ensure that contamination does not exceed prescribed limits.

DG-CWS-053. A capability shall be provided for maintaining the sterility of on-board water supplies.

DG-CWS-054. Water storage systems shall have provisions for isolating parts of the system which may have become contaminated.

DG-CWS-055. Water supplies shall be stored in areas which will minimize the possibility of contamination from other space station systems.

DG-INT-056. System components shall be designed to withstand the overpressure and heat pulse attendant to meteoroid penetration.

DG-ECS-057. Materials used for insulation or filler in space station walls shall be non-combustible.

DG-IFM-058. Windows shall be designed to permit replacement without degrading the pressure or structural integrity of the space station.

DG-STR-059. Individual habitable volumes shall be designed to withstand a rapid decompression of any adjacent compartment.

DG-STR-060. Space station structure shall be designed as a structural matrix with the capability of arresting crack and tear growth.

DG-INT-061. Equipment located in habitable volumes shall be designed to create no hazard to occupants during the changing environment associated with rapid decompression of the space station.

DG-MSE-062. Automatic closure of hatches between habitable volumes, when pressure decreases below a specified limit, should be considered as a design feature.

DG-OPS-063. Hatches between compartments should be closed except when required for crew transit.

DG-C&W-064. A means shall be provided for visual inspection of the hatch as well as the warning system, as a safety check to assure that hatches or other accesses to an area at a different pressure level have been secured properly. Warning system displays shall be at the hatch and at the command and control center(s).

DG-MSE-065. Pressure hatches providing access to an area of differential pressure should be of a type that becomes more positively engaged under pressure loading.

DG-ECS-066. Hatch design should be such that loss of a hatch seal element will not result in a pressure leakage rate which exceeds the emergency recompression system capability.

DG-INT-067. Provision should be made for an airlock in the hatch or hatchway between separately pressurizable compartments.

DG-INT-068. A leakage repair system employing techniques and equipment appropriate to the vacuum and gravity environment of the space station shall be provided as a kitable part of the damage control system.

DG-HMS-069. Consideration should be given to providing the equipment and supplies necessary for general cardiopulmonary resuscitation and other equipment and supplies that might be required for the individualized treatment of residual effects of decompression.

DG-FSE-070. All pressure relief valves shall be designed to protect against a regulator failed or stuck in the full open position.

DG-FSE-071. Plumbing systems which carry cryogenic fluids or hydrogen peroxide should be designed such that adequate pressure relief capability exists in those areas most likely to trap the fluids. Furthermore, to guard against the possibility that a relief valve in these systems becomes frozen shut or otherwise rendered inoperative, a backup pressure relief device, such as burst disks, should be incorporated.

DG-INT-072. All pressure systems should be designed to enable a planned depressurization; accurate sensors should be incorporated to ensure that the pressure is totally relieved prior to opening the system should that requirement arise for maintenance or other reasons.

DG-ECS-073. Any pressurizable volume than can be confined or isolated by any means, such as by valves, should include some means for automatic protection from overpressure.

DG-FSE-074. Pressurized gas supplies should include restrictions that will limit gas flow in the event of a pressurized gas plumbing failure, to that which can be handled by the relief valves or venting system.

DG-IFM-075. Design of space station structure and equipment, including their interfaces, should be such that all portions of the pressure shell, bulkheads and seals will be accessible for damage inspection and repair. This should apply to exterior as well as interior space station surfaces.

DG-INT-076. Potentially harmful effects on the crew members of rapid decompression should be minimized through engineering considerations in selection of space station atmosphere composition, pressure and habitable compartment net volume.

DG-STR-077. The space station shall be of sufficient structural strength to safely maintain the required internal pressure within the expected launch and mission environment for the period of orbital stay.

DG-IFM-078. Components which are vented to space (vacuum) shall be replaceable without requiring cabin depressurization.

DG-IFM-079. Cabin pressure shall not be vented to space through compartments or outlets that are used to vent fluids.

DG-ECS-080. Pressure relief devices for all pressurized volumes shall be vented to areas that will not endanger the crew or equipment.

DG-ECS-081. All cabin atmosphere overboard relief or "dump" valves (any valve venting into space) shall be fail-safe in the closed position and should be self-indicating when failed. Manual override or redundant manual valving should be provided as backup.

DG-C&W-082. Total cabin pressure sensors shall be provided to detect out-of-tolerance values of the total cabin pressure. Detection of pressure change at an excessive rate, or outside the desired operating range, should activate an alarm system to warn the crew to initiate appropriate remedial action. The alarm should be activated both in the affected habitable volume and at the command and control center(s).

DG-C&W-083. All pressure warning systems shall include provisions for self-test and shall be self-indicating in the failed state.

DG-EPD-084. Wire bundles shall be routed and protected as to preclude damage to the insulation through flexing or bumping.

DG-EPD-085. Suitable positive means, such as keying, shall be provided to preclude accidental mismatching of electrical connectors. This would be especially significant for connectors which are to be connected and disconnected during orbital operations (e.g., experiments).

DG-EPD-086. Consideration should be given to the design of electrical subsystem components (e.g., wall switches, light bulbs, or hot plates) to protect them from wear-out or inadvertent breakage, which could result in generating shorts or arcing.

DG-INT-087. Enclosed air duct systems that include potential sources of atmosphere contamination should provide sensors immediately downstream of the contamination source, which, if activated, would shut off the airflow through this equipment and provide a visual and audible alarm at the command and control center(s).

DG-ECS-088. Active redundancy should be provided for equipment which is essential to the control and detection of atmosphere contaminants.

DG-EPD-089. All temporary electrical connections (outlets, connectors, etc.) shall be so designed and/or operated as to eliminate the possibility of arcing.

DG-EPD-090. Wire bundles should not be located near potential heat sources, including those areas where potential for fire exists.

DG-EPD-091. Provisions should be made to ensure proper pin connection at all critical electrical connectors prior to the application of system power. Verification should be made to ensure that all pin connections exist as designed, no pin-to-pin shorts exist, and that no pin-to-shell shorts exist.

DG-INT-092. All equipment and substructure shall be grounded to the basic space station.

DG-INT-093. A means should be provided to equalize electric potential differences between docking spacecraft.

DG-EPD-094. Multiple power distribution paths to essential electrical equipment should be provided.

DG-C&W-095. Sensors shall be provided to detect out-of-tolerance values for critical electrical power source parameters, such as voltage, frequency, current, temperature, etc., or momentary excessive power surges resulting from equipment turn-on or turn-off. The sensors should activate an alarm system at the command and control center(s) of deviations from the desired parameters.

DG-EPG-096. Multiple or redundant primary electrical power sources shall be provided such that a single failure will not result in a complete loss of primary electrical power, or cause failure of equipment which is unable to survive momentary power interruption.

DG-EPD-097. Protective covers shall be provided for all portions of the electrical subsystem to which access is required (switch boards, terminal boards, etc.).

DG-EPD-098. Redundant electrical circuits for items critical to crew safety should not be included in the same wire bundle.

DG-EPD-099. Power distribution lines should be routed in such a manner that any damage resulting from fire, caused by a fault in the distribution system, will have a minimal effect on other power distribution wires in the vicinity.

DG-OPS-100. Procedures should be established and means provided the crew for controlling and/or eliminating contamination that is in excess of the ECS capability to control on a timely basis.

DG-ECS-101. Redundant CO2 removal equipment with capability of manual override of automatic operation should be provided to ensure a continuous capability to keep the CO2 partial pressure within allowable limits.

DG-ECS-102. The amount of toxic or potentially toxic materials (such as materials or chemicals utilized in experiments) on-board the space station should be limited such that accidental release of the total quantity of the material will not produce contamination above the capability of the environmental control system to remove on a timely basis.

DG-HMS-103. Threshold Limit Values (TLV's) of contaminants for long term human exposure should be established for space station environments.

DG-OPS-104. Strict configuration control procedures should be established over all materials incorporated in or brought on-board the spacecraft.

DG-OPS-105. The original orbital flight path selection and changes required by station-keeping during the mission should be such that the probability of collision with man-made debris or other spacecraft is sufficiently low to provide adequate confidence in orbit selection and program decision to proceed.

DG-CPH-106. All bulk cargo should be properly tethered or otherwise controlled during zero-gravity or partial gravity operations.

DG-OPS-107. Procedures and equipment should be available for use in event of death of a crew member.

DG-HMS-108. Procedures and equipment should be provided for the preservation or disposal of the remains of deceased experimental plants or animals.

DG-OPS-109. The program of selection, training, mission support, physical conditioning, daily activities, and recreation should insure that crew members remain confident in the mission and their roles in it.

DG-HMS-110. Procedures and equipment should be provided for restraint and control of irrational crew members.

DG-HMS-111. Unauthorized personnel should be restricted from using radiation-producing equipment or handling and using on-board radioisotopes. Consider the installation of appropriate caution signs and/or other means of warning, featuring visible or audible signals.

DG-HMS-112. Safe procedures should be established for the disposal of radioactive waste or radiation-contaminated material. The procedures should also include the actions necessary for the disposal of a spent or failed nuclear power reactor.

DG-HMS-113. On-board handling and use of radioactive material or radiation-producing equipment should conform or be consistent with established NASA and Nuclear Regulatory Commission policy and procedures for radiation protection standards.

DG-HMS-114. Positive protective measures should be taken to prevent accidental exposure to personnel from RF or X-radiation.

DG-EPG-115. Nuclear powered electrical power sources should be located and shielded to protect crew members from accumulating excessive radiation dosage.

DG-HMS-116. Crew location during the nuclear power unit activation should be restricted to refuge areas affording high protective shielding, until radiation levels have been checked in all habitable areas within the space station and have been found to be within acceptable limits.

DG-NUC-117. Space station installed/residing active nuclear reactor shall provide fail-operational/fail-safe measures for emergency shutdown of a reactor and provide alternate methods of reactor heat dissipation in event of failure of the primary cooling system.

DG-RSD-118. The space station radiation protection provisions shall be consistent with the orbital flight path type, orbital height, and inclination selected.

DG-CPH-119. Space station design and layout should make maximum use of any on-board mass as radiation shielding.

DG-RSD-120. Protection of the space station crew against the effects of a nuclear device explosion in space that releases radiation into the space station's orbital path should be considered.

DG-C&W-121. The location and characteristics of the radiation detectors should be consistent with the expected radiation environment.

DG-INT-122. Radiation effects upon space station electronic materials, microelectronic circuit elements, electrical systems, metals, ceramics, polymers, and other organic and inorganic materials should be thoroughly investigated for radiation-induced transient and permanent effects in terms of false signals, degradation, catastrophic failures, and contamination.

DG-OPS-123. In low-inclination (up to 60 degrees), low altitude orbits, Extra-Vehicular Activity should not be scheduled while the space station is passing through the South Atlantic Anomaly. For polar orbit, the same guideline applies. In addition, the occurrence of a solar event should require that EVA be avoided.

DG-OPS-124. A mission radiation control program should be instituted to develop radiation exposure limits, procedures, design criteria, and responsibilities consistent with the expected mission environment and period of orbital stay.

DG-HMS-125. A cumulative radiation exposure record should be kept on each crew member, and personnel who have reached the limit of safe radiation exposure should be returned to earth without delay.

DG-INT-126. Provision should be made in the space station for a designated shelter that would serve as a haven for radiation protection against possible high-intensity radiation events. This shelter should contain the necessary life support equipment and provisions consistent with the maximum expected stay time for the particular mission profile.

DG-HMS-127. Space station radiation monitoring, including cumulative radiation level records, should be maintained to ensure the precise determination and provide clear notification of radiation conditions, and warning of possible over-irradiation of the space station.

DG-C&W-128. The space station detection system should continuously monitor the interior and exterior radiation levels and record the accumulated dosage for the mission.

DG-RSD-129. Additional protection for crew members performing EVA in the proximity of a nuclear power source should be provided.

DG-INT-130. Precautions should be taken in the selection of spacecraft materials to ensure that the materials will not support induced radiation.

DG-OPS-131. Maintenance procedures for CO₂ control equipment should take into account the possible high operating temperatures of the equipment and the possibility of release of contaminants.

DG-OPS-132. The storage and disposal of combustible waste materials should be such that a fire hazard or traffic obstruction is not created.

DG-INT-133. Flame arrestors should be provided in all ducting through which flame could propagate.

DG-INT-134. Cryogenic piping systems should provide for both automatic and manual emergency shutoff.

DG-EPG-135. Adequate cooling capability should be provided to prevent overheating of electrical power sources even during worst-case conditions.

DG-INT-136. Power generating and distribution equipment which is a potential source of fire should be located in unpressurized areas in the space station.

DG-INT-137. Fire control equipment and/or methods should be provided which can be automatically initiated, or are readily accessible and can be manually controlled.

DG-INT-138. Electrical insulation should be, as a minimum, self-extinguishing in the space station atmosphere.

DG-INT-139. Power equipment racks and cables should be as resistant to fire as possible. Emergency equipment and casualty mode/damage control operations should be developed.

DG-INT-140. All fluid lines should be adequately protected from freezing due to proximity to cryogenics, or exposure to black space.

DG-INT-141. Heating elements which must be exposed to the atmosphere should be provided with a device to prevent the propagation of flame.

DG-C&W-142. Areas where radioactive materials are used or stored should be monitored for radioactive contamination, and suitable warnings provided if radioactivity exceeds established limits.

DG-INT-143. Components which could generate excessive heat due to friction should be automatically monitored for temperature increase and sealed from the atmosphere. An overheat warning signal should be provided.

DG-INT-144. The amounts of hypergolic, pyrophoric, or other easily ignitable materials on board the space station should be restricted to the minimum necessary, and close control should be exercised over their handling and use.

DG-INT-145. Potential ignition sources, such as lighted cigarettes or open flames, etc., should not be permitted within the pressurized inhabited compartment of the space station unless rigid control can be exercised to insure that a fire hazard is not present.

DG-INT-146. If absence of oxygen is utilized as a means of preventing fires, design should provide that no single failure could produce an oxygen atmosphere.

DG-INT-147. Passageways should be kept free of all combustible materials and oxidizers.

DG-MSE-148. Lubricants used in mechanical components which are essential for survival should be capable of withstanding extreme temperatures.

DG-ECS-149. A capability for manually controlling operation of equipment used for cabin and equipment temperature control should be considered.

DG-EPD-150. Current limiting devices or techniques should be used to preclude hazardous overcurrents. Devices should be readily accessible, provide visible indication of their state, and be resistant to inadvertent or accidental de-activation, fire, explosion, shock and explosive decompression. They should provide protection both to the current source and to the "using" equipment.

DG-INT-151. Design provisions should be made which assure that no heated surfaces would provide a source of injury to crew members or provide a source of ignition.

DG-FSE-152. Propellant supply system equipment and plumbing which uses toxic or potentially flammable fluids should be located in uninhabited areas.

DG-INT-153. Equipment which has a critical temperature requirement should be protected by redundant or alternate temperature control capability.

DG-INT-154. Materials which are capable of self-propagation of fire should not be on-board the space station in sufficient quantities or concentrations that ignition would result in a hazardous condition.

DG-ECS-155. Valves for oxygen systems of 3000 PSI or higher should be slow opening and closing to minimize the possibility of ignition of contaminants.

DG-ECS-156. Space station thermal protection provisions should be consistent with the orbital flight path, orbital height, and inclination selected.

DG-ECS-157. Thermal control equipment whose operation is critical to crew safety should have redundancy provided.

DG-ECS-158. Temperature sensors should be provided at critical points in thermal control systems to detect out-of-tolerance temperatures. Detection of temperatures which deviate from the normal range should activate an alarm system to warn the crew of the need for remedial action.

DG-INT-159. Procedures should be established and design safeguards provided that will preclude operation of thrusters when it might endanger crew members involved in EVA.

DG-AOM-160. Sensors should be provided to monitor the temperature of attitude control thruster assemblies. The sensors should activate visual and/or audible alarm at the command and control center(s).

DG-AOM-161. Angular rates of the space station should be continuously monitored during attitude change maneuvers. Detection of excessive angular rates should result in automatic/controlled shutdown of operating thrusters.

DG-AOM-162. An automatic system for controlling thrusters to restore a tumbling space station's stability should be provided.

DG-AOM-163. Redundancy should be provided for all components that are located outside pressurized inhabited areas and failure of which could result in a loss of attitude control.

DG-AOM-164. The attitude maintenance system should have the capability to counteract the undesired motion imparted by fluid escaping through a hole in a compartment or pressure vessel.

DG-AOM-165. Interlocks should be provided to prevent simultaneous manual and automatic operation of the attitude control system.

DG-AOM-166. A means for stopping propellant flow to failed OPEN thrusters should be provided.

DG-INT-167. Outlets should be designed so that fluids being vented overboard do not impose any torque on the spacecraft.

DG-FSE-168. Propellants should be stored in more than one tank or other storage device.

DG-INT-169. Accessways between and within compartments should be sized in such a manner that an IVA-suited crew member will be allowed to access to normally used areas.

DG-STR-170. Hatches should be capable of being operated from either side and at least two methods for operating the hatches should be provided.

DG-ECS-171. Space station airlocks should have redundant pressurization capability.

DG-INT-172. An alternate command and control center should be provided in the space station, possibly within the crew refuge area, to ensure continuation of a minimum number of functions which are vital for base control and crew life support, in the event the primary command and control center is rendered incapable of providing these functions.

DG-INT-173. Capability should be provided to allow entry into a compartment, where fire or other emergency exists, to effect rescue of incapacitated crew members or to combat a fire. The means of entry and the procedures involved should assure that the emergency does not escalate or spread to other locations in the space station.

DG-OPS-174. Mission rules should include the requirement that control center "authority to proceed" be obtained immediately prior to the initiation (by any crewmember) of any activity which is hazardous either by itself, or when performed in conjunction with other base activities being conducted simultaneously.

DG-C&W-175. Closed circuit television system with strategically located cameras should provide command and control center operator(s) real-time visual information on hazardous activities/operations.

DG-OPS-176. Simultaneous occupancy (other than momentary) by the space station commander and his deputy, of those compartments or locations which are judged to have the highest safety risk probability, should be minimized.

DG-COM-177. Equipment in the space station for external voice and data communications should have as much commonality as practicable with the equipment used in the logistics vehicles and earth-return vehicles.

DG-AOM-178. Continuous indication of space station attitude or attitude changes should be provided to the command and control center(s).

DG-OPS-179. Crew activity should be restricted during transfer of volatile, flammable, or explosive materials either between docked spacecraft, the logistics vehicle, or within the space station. These restrictions should apply to the use of high voltage equipment, conduct of high temperature experiments, or other activity which would involve a potential source of ignition in the immediate neighborhood of the material transfer route.

DG-OPS-180. The number of crew members in any compartment at one time should be held to a minimum necessary to perform the required functions.

DG-OPS-181. Crew members should be restricted from movement about the station other than within specified and assigned areas.

DG-INT-182. The areas in which the crew spends most of its time (staterooms, dining facilities, personal hygiene areas, exercise and recreation areas) should be designed as the safest parts of the space station.

DG-C&W-183. Critical visual/audible C&W alarms should be displayed in all inhabited compartments.

DG-COM-184. An independent emergency communications system should be provided for directing and controlling operational activities in emergency situations.

DG-OPS-185. A sufficient number of logistics and/or rescue vehicles should be docked to the space station at all times to accommodate every on-board crew member in the event that emergency evacuation is required.

DG-COM-186. Independent emergency communications should be provided to assist EVA personnel in performing their tasks or to facilitate rescue of EVA personnel.

DG-EPD-187. Emergency lighting system should be provided to assist EVA personnel in performing their task or to facilitate rescue of EVA personnel.

DG-OPS-188. Periodic drills for all personnel should be devised, and conducted in response to unscheduled simulated emergencies, so that crew proficiency is maintained in emergency procedures.

DG-OPS-189. "Fire Resistant" areas should be established to provide haven from fire. Emergency procedures should be established to identify such things as optimum routes to haven from any area, and all personnel should be trained in these procedures.

DG-OPS-190. Procedures should be established and training provided to the crew which will enable them to cope with any foreseeable contingency that might arise during EVA.

DG-C&W-191. An adequate fire warning system should be provided. The warning should be activated by smoke or fumes, as well as heat, and should warn the entire space station. The precise location of the fire should be provided to the command and control center(s). All segments of the warning system should be resistant to temperature extremes, decompression/overpressure or shock and should be self-indicating when failed.

DG-FSE-192. A means for monitoring fluid quantity usage should be provided to permit the crew to detect excessive consumption rates and low remaining supply levels.

DG-C&W-193. The commencement, behavior, and completion of all remote hazardous resupply operations (pressurized liquid or gas resupply) should be positively indicated at the command and control center(s).

DG-OPS-194. Overall health and safety responsibilities should be assigned to specific members of the crew with alternates.

DG-OPS-195. Procedures should include the provisions for abort for all incoming vehicles having an on-board emergency which would jeopardize the space station.

DG-EPG-196. An emergency power source which is completely independent of the primary power source should be provided.

DG-OPS-197. An initial advanced manning team should check habitability of the space station prior to duty crew manning.

DG-COM-198. A visual warning should be provided to the command center(s) when any link of the space station communication system fails.

DG-COM-199. At least one intercommunications station should be provided for each separately pressurizable space station compartment that can be occupied by the crew.

DG-INT-200. The maintenance equipment, procedures and skills required to completely analyze and isolate component failures and accomplish the needed replacement or repair should be provided.

DG-C&W-201. Critical subsystems of docked transient vehicles should be continuously monitored in the space station command and control center(s), with appropriate warnings for out-of-tolerance conditions.

DG-OPS-202. All EVA and IVA suited activities shall be backed up and monitored by a suited crew member who is in a position to provide immediate assistance.

DG-OPS-203. A periodic, two-way communications check should be made by the command and control center with all elements that comprise the space station. A "no communications" period would automatically initiate space station emergency procedures.

DG-OPS-204. Armable subsystems that comprise the space station and its docked vehicles should be armed only when they are to be used and immediately disarmed when their function is no longer required.

DG-INT-205. The pressurized compartments of a space station should have adequate free volume (not occupied by equipment or structure) to provide the crew freedom of movement and a psychological and physiological environment that is commensurate with their orbital stay duration.

DG-C&W-206. Leak detectors should be provided for propellant handling equipment located in unpressurized areas of the space station. The detectors should activate an alarm at the command and control center(s).

DG-INT-207. Replacement components should be designed so that it is impossible to inadvertently install the component incorrectly.

DG-INT-208. Universally sized, minimum time to don or place, survival devices should be made available to the crew.

DG-INT-209. All switches should be designed and located so that the possibility of inadvertent activation or improper selection is minimized.

DG-MSE-210. Design of mechanisms shall minimize the number of moving parts or other maintenance task generators.

DG-FSE-211. Small clearances in fluid system should be avoided where fluid entrained particulants could cause binding or jamming of system components.

DG-STR-212. Hatch design shall avoid seal abrading in normal operation.

DG-STR-213. Provisions shall be made for moisture removal between transparency panes.

Appendix BE
SPACE STATION HAZARD LIST

The enclosed list of 148 candidate space station hazards are included to indicate some typical safety concerns. This list is neither official nor all inclusive, but is submitted to indicate the scope of hazards to be considered. A similar list will be generated within each jurisdictional area (agency/contractor), aggregating the hazard report titles from the safety assessment process noted in Appendix AF. When the Space Station electronic network safety data base comes on-line, this appendix will be a printout of the space station hazards list.

9 MAR 83

SPACE STATION CANDIDATE HAZARD LIST

- 001 Debris Impairing Mechanism Functioning
- 002 Entrapment of Combustible Fluids
- 003 Failure of Docking Separation Mechanisms
- 004 Failure of Servicing Separation Mechanisms
- 005 Contained Systems Overpressure
- 006 Inadvertent Thruster Firing
- 007 Inadvertent Command (Manual/Software) Actuation
- 008 Ingress/Egress Hatch Mechanism Failure
- 009 Heat Exchanger Coil Rupture
- 010 Hazardous Fluid Leakage
- 011 Thruster Premature Shutdown
- 012 Thruster Failure to Fire
- 013 Pressurized Tank Explosive Rupture
- 014 Insufficient Remaining Propellant
- 016 Battery Thermal Runaway
- 017 Failure to Key Connectors
- 018 Use of Wet Tantalum Capacitors
- 019 Momentary Power Interrupt
- 020 Power Transients
- 021 Loss of Gyro Stability
- 022 Loss of Guidance System Accuracy
- 023 Corona and Arcing
- 024 EVA Crewman Irradiation

9 MAR 83

- 025 Failure of C&W System to Alert Crew
- 026 Erroneous Alarm
- 027 CO2 Level not Annunciated
- 028 Single Fault in Computer Systems
- 029 Inadequate Locking of Connectors
- 030 Failure to Deadface Guillotine Circuits
- 031 Mating/Demating Connectors with Power Applied
- 032 Unknown Relay State in Startup
- 033 Damage Susceptibility to Wiring Harness
- 034 Payload Deploy/Retrieve Loss of Power/Control
- 035 Power Interrupt Causes Computer Shutdown
- 036 EMP Disabling Critical Semi-Conductor Circuitry
- 037 Loss of Avionics Colling
- 038 Loss of Compartment Air Control
- 039 O2/N2 Tank Explosion
- 040 Free Water Short in Electrical Equipment
- 041 Contamination of Potable Water
- 042 Fire Suppression System Fails to Extinguish Fire
- 043 Non-Restraint of Crewman Using Portable Fire Extinguisher
- 044 Loss of Airlock Life Support
- 045 Loss of Access to "Safe Haven"
- 046 Fire in Habitable Compartment
- 047 Corrosive Fluid Spills in Habitable Compartments
- 048 Leaking of Hazardous Fluids During Fluid Transfer
- 049 Contamination by Radiative Materials
- 050 Contamination by Chemical/Biological Contaminants

9 MAR 83

- 051 Inability to Isolate Critical Function
- 052 Pressure Shell Penetration From Shrapnel
- 053 Collision of High Mass Objects with Space Station
- 054 Sharp Edges and Corners
- 055 Hypoxia in a 10.2 PSIA Atmosphere
- 056 Inadequate Monitoring and Override of Automatic Functions
- 057 Collision between Orbiter and Space Station
- 058 Collision between OTV and Space Station
- 059 Space Station Collision with Space Debris
- 060 No Exit from Habitable Volume
- 061 Delayed Reaction to Emergency EVA
- 062 Non-Ionizing Radiation Interference
- 063 Inability to Transfer to Rescuing Orbiter
- 064 Space Station Orbit Decay
- 065 Loss of Pressurization in Adjacent Module During Docking/Undocking
- 066 Loss of Life Support During/After Emergency
- 067 Space Station Spinup from Assymetrical Venting
- 068 Cross Contamination of Habitable Volumes
- 069 Compartment Overpressurization from Heat/Fire
- 070 Undetected Fluid Leaks and Pressure Loss
- 071 Hazardous Materials in Habitable Volumes
- 072 Radiation Levels Exceeding Allowables
- 073 Efflux Impingement on Space Station
- 075 Poor Space Station Housekeeping
- 076 Inability to Inspect Tie Down Restraints

9 MAR 83

- 077 Near Space Station Container Explosion/Rupture
- 078 Combination of Mutually Reactive Fluids in or near Space Station
- 079 Monopropellant Decomposition or Leakage in or near Space Station
- 080 Inadvertent Start of Upper Stage Rocket Motor in Vicinity of Space Station
- 081 Collision of Loose Upper Stage Parts with Space Station
- 082 Loss of Control of Upper Stage in Vicinity of Space Station
- 083 Inability to Dock Upper Stage to Space Station
- 084 Inability to Dock Orbiter to Space Station
- 085 Contaminated Space Station Equipment and Crew
- 086 Glare Blanking of Remote Video Cameras
- 087 Protrusions into High Traffic Areas
- 088 Hatch Blow-In from Inter-Volume Pressure Differentials
- 089 Inability of Critical Subsystems to Withstand Habitable Volume Depressurization
- 090 Propagation of ECS Failure to Other Habitable Volumes
- 091 Smoke Inhalation
- 092 Food Poisoning
- 093 Inability to Treat Crew Illnesses/Injuries
- 094 Disposition/Handling of Crew Member Remains
- 095 Crew Member Chronic Motion Sickness
- 096 Berserk Crewman
- 097 Crewman Illness on EVA

9 MAR 83

- 098 Spread of Pathogenic Bacteria Through Crew Personal Effects
- 099 Free Floating Internal Debris
- 100 Undesired Electrolytic Corrosion
- 101 Tumbling Astronaut (EVA)
- 102 Tumbling Astronaut (IVA)
- 103 Breakdown in Crew Discipline/Jurisdiction
- 104 Ergonomic Stresses
- 105 Deterioration of Maintenance/Repair Quality Control
- 106 Exposure to Excessive Noise 60 dB(A)
- 107 Toxic Vapors, Gases, Metals
- 108 Exposure to Temperature Extremes
- 109 Electric Shock
- 110 Fluid Line Contamination
- 111 Vector (Insect/Rodent) Control
- 112 Ozone Generation in Habitable Volumes
- 113 Non-Maintainable Subsystems
- 114 Contamination from Waste Products
- 115 Common/Interconnected Water Supply
- 116 Crack Propagation in Structures and Lines
- 117 Flying Debris Caused by Rapid Decompression
- 118 Habitable Volume Rapid Decompression
- 119 Hatch Seal Leakage
- 120 Trapped Fluids
- 121 Inability to Inspect Primary Structure
- 122 Electrical Connector Mismatch
- 123 Arcing of Electrical Components

- 124 Wiring Harness Shorts
- 125 Electrostatic Discharge
- 126 Spacesuit Burnthru from Hot Utility Lights
- 127 Rotating Machinery Run Away
- 128 Interconnection of Lines at Different Pressure Levels
- 129 Rupture of High Pressure Lines
- 130 Water Electrolysis Unit Cell Reversal
- 131 Chemical/Thermal Burns to Crew Members
- 132 Communicable Disease Outbreak
- 133 Death of Crew Members
- 135 Death of Experimental Plants/Animals
- 136 Excess O₂ Partial Pressure
- 137 Nuclear Contamination
- 138 Irradiation of Crew and Equipment
- 139 Freezing/Disassociation of Lubricants in Space Environment
- 140 Violation of Critical Equipment Environmental Requirements
- 141 Loss of Command/Control Capability
- 142 Loss of Inter-Volume Communication
- 143 Loss of Space Station-to-Ground Communications
- 144 Loss of Internal Illumination
- 145 Undefined Escape Routes
- 146 Depletion of Critical Consumables
- 147 Inadequate Spares Provisioning
- 148 Crew Congestion at Work Stations

This Page Intentionally Left Blank

1. Report No. NASA CR-3858		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Space Station Crew Safety Alternatives Study - Final Report. Volume V - Space Station Safety Plan				5. Report Date June 1985	
				6. Performing Organization Code	
7. Author(s) G. H. Mead, R. L. Percy, Jr., and R. F. Raasch				8. Performing Organization Report No. SSD84-0055	
9. Performing Organization Name and Address Rockwell International Space Station Systems Division 12214 Lakewood Blvd. Downey, Ca. 90241				10. Work Unit No.	
				11. Contract or Grant No. NAS1-17242	
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Washington, DC 20546				13. Type of Report and Period Covered Contractor Report	
				14. Sponsoring Agency Code 906-54-02	
15. Supplementary Notes Langley Technical Monitor: Robert D. Witcofski Final Report					
16. Abstract The Space Station Safety Plan has been prepared as an adjunct to the subject contract final report, suggesting the tasks and implementation procedures to ensure that threats are addressed and resolution strategy options identified and incorporated into the space station program, such that minimum risk exposure to the space station personnel and resources is realized.					
17. Key Words (Suggested by Author(s)) Threats, Hazards, Strategies, Safety Assessment, Human Factors, Safety Criteria, Safety Guidelines, Safety Tasks			18. Distribution Statement Unclassified - Unlimited Subject Category 15		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 116	22. Price A06

National Aeronautics and
Space Administration

Washington, D.C.
20546

Official Business

Penalty for Private Use, \$300

SPECIAL FOURTH CLASS MAIL
BOOK

Postage and Fees Paid
National Aeronautics and
Space Administration
NASA-451



NASA

POSTMASTER: If Undeliverable (Section 158
Postal Manual) Do Not Return
