Bendix

Aerospace Systems Division

SYSTEM SAFETY PROGRAM PLAN FOR ALSEP FLIGHT ARRAY E

NO.	REV. NO.
ATM 935	
PAGE 1 OF 18	
DATE 1-11-71	

This plan establishes the System Safety requirements for the ALSEP Flight Array E, except for the more extensive requirements for Lunar Seismic Profiling (LSP) Experiment which are established in ALSEP-LS-10.

Prepared by: Joseph R. Jones

Joseph R. Jones
System Safety Engineer

Approved by: B. J. Rusky

B. J. Rusky, Manager
ALSEP SYSTEM SUPPORT

1. PURPOSE

The purpose of this document is to informally establish the system safety requirements for the ALSEP Flight Array E. The objectives of this plan are to determine, by systematic methods of analysis, the degree of safety attained in the final product delivered under this contract and to document the methods, scope of activities, and criteria used in making this determination to the extent required by the contract.

Formal System Safety Program requirements for the Lunar Seismic Profiling Experiment are identified in Reference 2.11, below.

2. REFERENCES

This plan has been derived from the requirements, methods, and intent presented in the documents which are listed below for reference only:

2.1 NASA Office of Manned Space Flight, "Safety Program Directive Number 1A"

2.2 Air Force System Command Design Handbook 1-6, "System Safety".

2.3 NASA Safety Manual, NHB 1700.0 (VI), Volume I, "Basic Safety Requirements".

2.4 U.S. Army Missile Command, RK-TR-62-10, "Safety Considerations with Electroexplosive Devices" 26 November 1962.

2.5 NASA KSC K-V-053 "APOLLO/SATURN V Ground Safety Plan".

2.6 NASA KSC KMI 1710, "The KSC Safety Program".

2.7 Air Force Eastern Test Range AFTRM 127-1 "Range Safety Manual".

2.8 NASA MSC, MSCM 8080 "Manned Spacecraft Criteria and Standards".

2.9 NASA MSC Safety Office "Attachment G System Safety Requirements for Manned Space Flight Experiments," 12 September, 1969.

2.10 NASA Apollo Reliability and Quality Assurance Office, RA-006-013-1A, "Procedures for Failure Mode, Effects, and Criticality Analysis (FMECA)" August 1966.

2.11 BxA, ALSEP-LS-10, "System Safety Plan for ALSEP Flight Array E Lunar Seismic Profiling Experiment Subsystem".

3. HAZARD CATEGORIES

Hazard categories are established to assure that potentially hazardous systems or associated procedure identified by the hazard analysis receive appropriate attention. Hazards shall be placed in the appropriate hazard category as they are identified.

3.1 Safety Catastrophic - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem or component malfunction will cause death or injuries to personnel.

3.2 Safety Critical - Conditions(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem or component malfunction will cause a hazard which requires immediate corrective action to avoid loss of or injury to personnel.

3.3 Safety Marginal - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem failure or component malfunction will degrade system performance but which can be counteracted or controlled without major damage or any injury to personnel.

3.4 Safety Negligible - Condition(s) such that personnel error, design characteristics, procedural deficiencies, subsystem failure, or component malfunction will not result in major systems degradations, and all not produce system functional damage or personnel injury.

4.1 SYSTEM SAFETY PLAN (SSP)

The following paragraphs delineate the SSP as an integrated effort within the ALSEP Program:

4.1.1 Organization

System Safety is a recognized engineering discipline within the BxA Systems Engineering Department. It embodies special techniques of analysis and management developed in recent years within the Aerospace Industry which, when applied to a system under development, assure a detached and impartial evaluation of the level of safety attained, which facilitate the identification of potential safety problems at a point in time in the development cycle when they can be most economically resolved, and which establish specific responsibility for safe performance.

The ALSEP System Safety Engineer reports to the ALSEP System Support Manager. He is responsible for the preparation and execution of the System Safety Plan and serves as the single point of contact for matters relative to safety. He maintains direct contact with the BxA Health and Safety Officer and with customer and associated contractor safety elements. The functional relationship of the System Safety Engineer to other program elements is presented in Figure 4-1. The schedule of activities to be accomplished in the execution of this plan is presented in Figure 4-2.

4.1.2 Management and Control

The methods and rules to be utilized in the implementation and management of the SSP are established in the following work statement items:

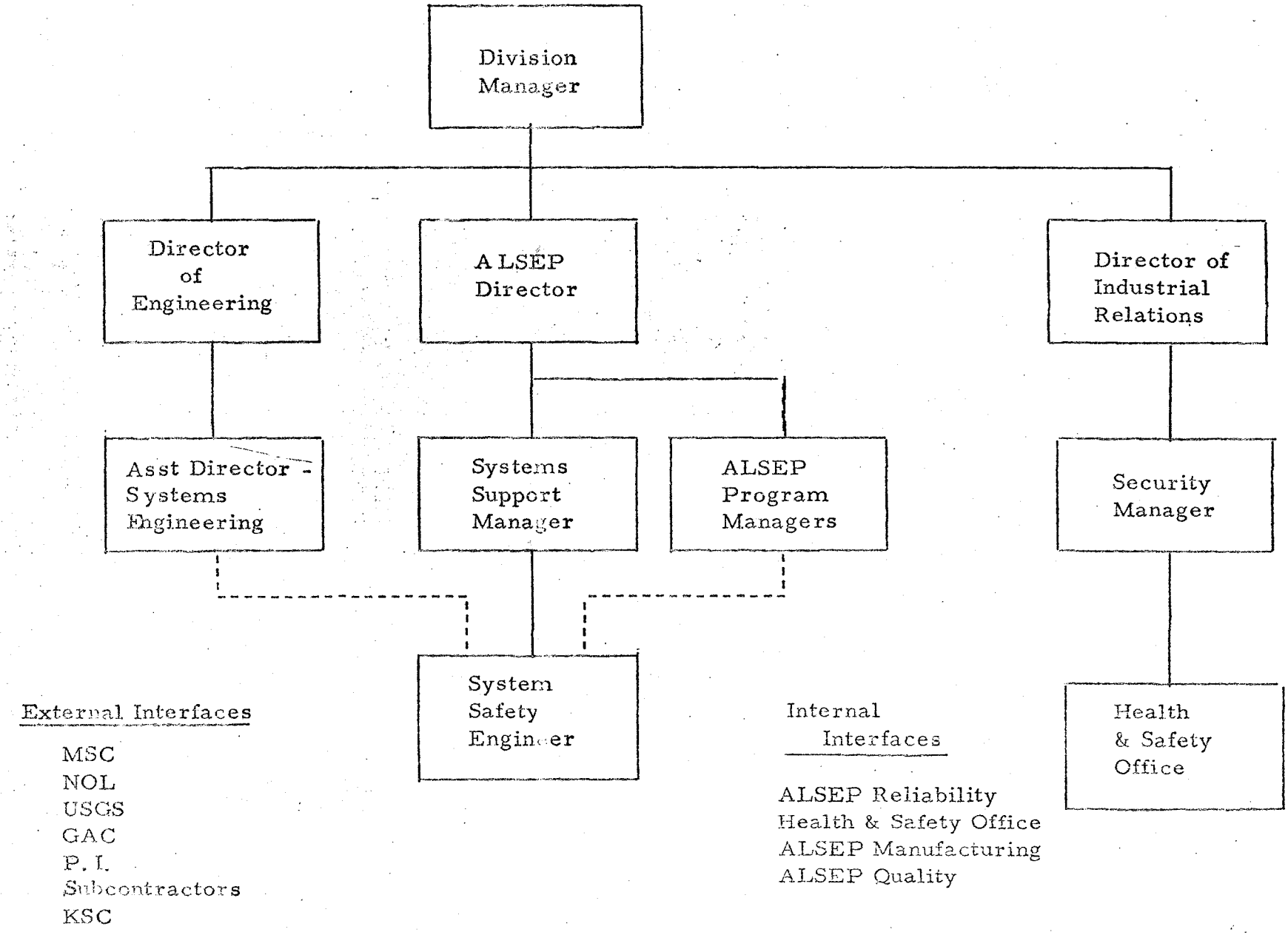

Figure 4-1 ALSEP System Safety Engineering Functional Organization Chart

Bendix Aerospace Systems Division

SYSTEM SAFETY MASTER SCHEDULE

ALSEP Flight Array "E"

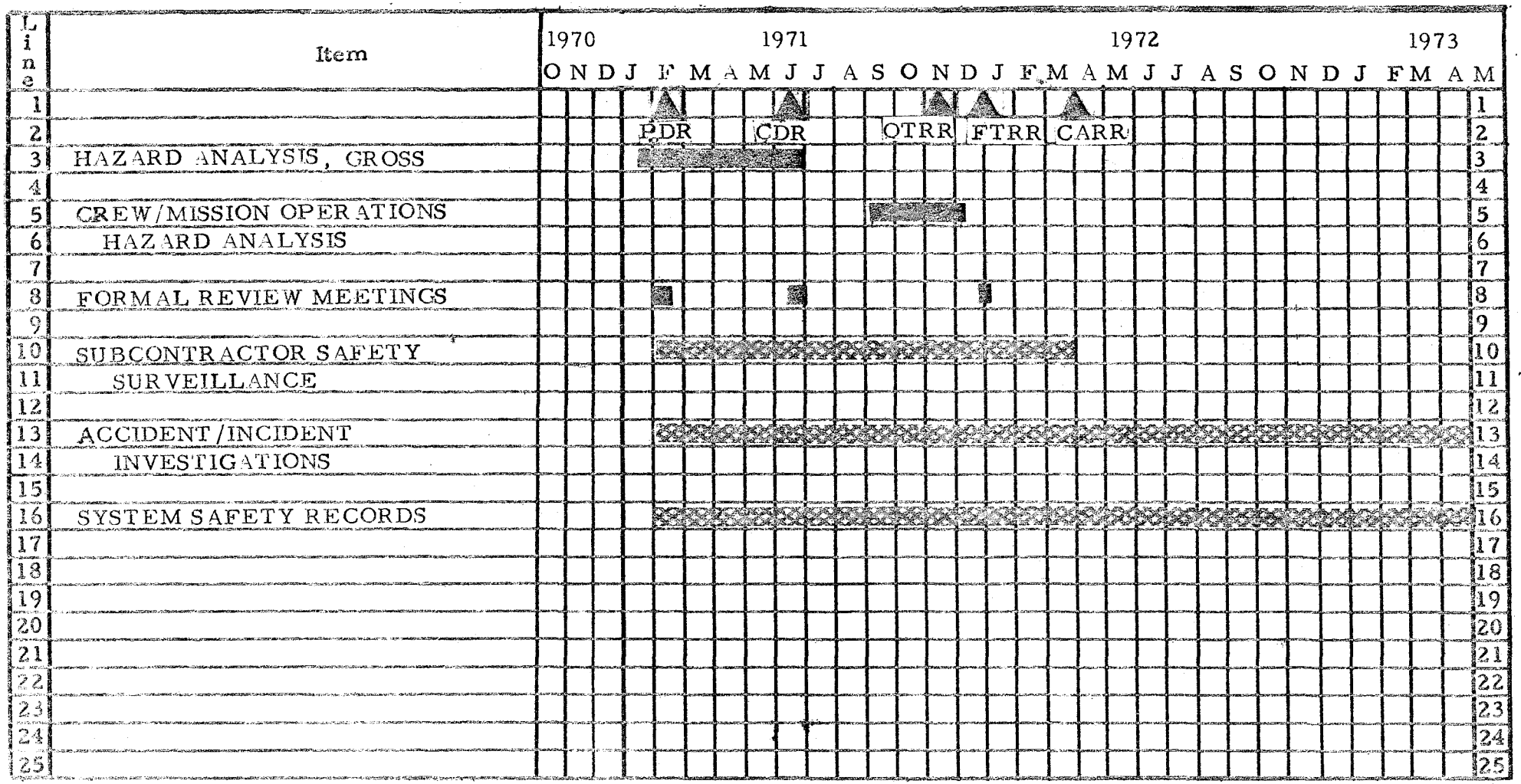

FIGURE 4.2

4.1.2.1 System Safety Program

System Safety shall be given prime consideration in all policies, engineering designs, and plans related to the ALSEP Array E.

4.1.2.2 System Safety Participation in Formal Reviews

The System Safety Engineer shall attend selected formal Program System Level Review meetings held at BxA as noted in Figure 4-2 and shall be prepared to present the status of SSP activity, significant accomplishments since the previous review, and his assessment of the problems yet to be resolved in the completion of scheduled activities.

4.1.2.3 System Safety Records

Records pertaining to System Safety activities on the program shall be centrally maintained in the custody of the System Safety Engineer. The filing system shall be established to faciliate the retrieval of safety documentation in an orderly manner for audit and review by MSC Representatives.

4.1.2.4 Evaluate and Assess Safety Problems

Safety problems shall be evaluated and assessed as part of the overall hazard analysis and reporting activities described in paragraphs 4.2 and 4.4.

4.1.2.5 Accident/Incident Investigations

The System Safety Engineer shall participate in the investigation of accidents and incidents involving the ALSEP Array E and shall be responsible to see that necessary corrective action taken is adequate from a safety viewpoint. Additional information on the requirements for accident and incident reporting is contained in paragraph 4.4.3.

4.1.2.6 FMEA Identified Category Hazards and Single Point Failures

FMEA results identifying Category I (as defined in paragraph 2.2.10) elements and single point failures shall be identified as potential hazards and shall be incorporated into the hazard analyses conducted within the requirements of this SSP for assessment, reduction on control and for development of such risk criteria as may be appropriate.

4.1.2.7 Subcontractor System Safety

SSP's shall not be required of subcontractors. System Safety surveillance over subcontractor activities shall be through the LSPE project engineering organization and analyses shall be performed as may be required as part of the overall hazard analysis effort.

Subcontractors shall not be required to submit accident/incident reports to the contractor in accordance with the criteria established in paragraph 4.4.3. However, any significant condition noted during routine system safety surveillance of subcontractor activities shall be documented and processed by the System Safety Engineer in the same manner as any accident/incident originating within the BxA facility.

The System Safety Engineer shall review proposed subcontract specifications and, if more specific requirements are not appropriate, shall recommend that the following statement, with modifications as may be appropriate to the particular specification, be included as a basic safety requirement.

"Safety Requirement - The design shall preclude, either through elimination of causes or the incorporation of protective methods or devices, the possibility of physical harm or injury from the hazardous effects of sharp edges and corners, the discharge of electrical energy, the stored energy of compressed gases, springs, and other devices, the effects of chemical processes utilized within the equipment, the effects of radiated energy or the transfer of heat to the external surroundings, or from accidental contact with voltages in excess of 30 volts, root mean square or direct current, during normal operation or maintenance of the equipment.

Accidents, incidents or other observations relating to the design, operation or other unique condition of the equipment which is indicative of a potential problem or hazardous situation beyond the scope of the subcontractors responsibility to resolve shall be reported to BxA."

4.2 HAZARD ANALYSIS

4.2.1 Gross Hazard Analysis

A gross hazard analysis will be performed for each Array E Subsystem during the initial design phase to identify potential problems which could impact the safety of the crew.

The analysis will utilize preliminary design layouts, logic diagrams, preliminary failure modes and effect analysis and any other available information which helps to define the proposed engineering design. The depth of the analysis performed will be limited by the level of information available, but will be designed for maximum effect in uncovering inherent hazards which may exist at an early point in the preliminary design cycle and in establishing a level of safety confidence from which detail design and procurement activities may proceed.

4.2.2 Crew/Mission Operations Hazard Analysis

The Crew/Mission Operations Hazard Analysis extends the safety analysis beyond the Engineering Design and in particular will ensure that mission rules and crew procedures are adequate for potential experiment problems. A study will be conducted of all manually initiated experiment commands to determine the potential for error and the effects of such errors.

4.2.3 Hazard Analysis Procedures

4.2.3.1 General Procedure

The starting point for a hazard analysis is the Preliminary Hazard Analysis Checklist (Figure 4-3). This list provides a convenient and systematic approach to identifying and recording the potential hazards which may be pertinent to a particular component or operational technique in the major functions of the system during various phases of operation. The checklist is not intended to be restrictive in nature and may be expected to open areas of concern beyond the boundaries suggested by the format.

As the hazard analysis sheets are completed, a preliminary hazard list may be extracted from them and analyzed by phase, function and component utilizing the System Safety Problem Sheet (Figure 4-4) as a convenient and permanent record.

As potential hazards are analyzed and requirements for control or corrective action are identified, they are entered on the System Safety Record Sheet (Figure 4-5), in which format they will be published in the hazard analysis reports. A positive statement is required on the record sheet to indicate how the identified hazard will be eliminated or controlled.

4.2.3.2 Input Data

Input data for the hazard analyses may come from the following sources and from such other sources as may be useful and available:

Engineering Drawings

Engineering Trade-off Studies and Reports

Test Plans and Procedures

Test Results

End Item Specifications

Materials Lists

Failure Mode and Effects Analysis

Configuration Specifications

Subcontract Specifications

Failure & Unsatisfactory Condition Reports

Failure Analysis & Corrective Action Reports.

Bendix
Aerospace Systems Division
SYSTEM SAFETY ENGINEERING

PRELIMINARY HAZARD ANALYSIS SHEET
ALSEP ARRAY E

SYSTEM _____ BY _____
COMPONENT _____ DATE _____
DETAIL/ASSEMBLY/OPERATION _____

HAZARD / PHASE	MANUF & TEST	FIELD TEST	KSC	LAUNCH & LANDING	LUNAR SURFACE	REMARKS
ACCELERATION						
AERODYNAMIC LOADS						
AERODYNAMIC HEATING						
CHEMICAL						
CONTAMINATION						
CONTROL SYSTEM FAILURE						
COLLISION						
CORROSION						
DEBRIS						
DEHYDRATION						
EGRESS						
ELECTRICAL-INADVERTENT ACTIVATION						
ELECTRICAL-POWER SOURCE FAILURE						
ELECTRICAL SHOCK						
ENDURANCE LIMIT EXCEEDED						
ENVIRONMENTAL STRESS						
EQUIPMENT FAILURE						
EXPLOSION						
EXPOSURE						
FIRE						
FRAGMENTATION						
HEAT & TEMPERATURE						
IMPACT						
INSTABILITY						
LEAKAGE						
LIFE SUPPORT SYSTEM FAILURE						
MOISTURE						
OXIDATION						
OFF COURSE						
PERSONNEL ERROR						
PERSONNEL ILLNESS						
PRESSURE						
PROPULSION FAILURE						
RADIATION						
RESCUE CAPABILITY						
SHOCK						
SMOKE						
STRESS CONCENTRATIONS						
STRESS REVERSALS						
STRUCTURAL FAILURE						
TOXICITY						
VIBRATION AND NOISE						
WEATHER						

Aerospace Systems Division

SYSTEM SAFETY PROBLEM SHEET

_____ of ____

Program _____

Task _____

Analyst _____

ROBLEM

1. COMPONENT FAILURE OR DEFECT
2. CREW OR GROUND PERSONNEL ERROR
3. CREW IMPAIRMENT

ISSION RISKS

1. UNPREDICTABLE EVENTS
2. "EXPECTED" LOW PROBABILITY EVENT OR FAILURE
3. OPERATIONAL ENVIRONMENT
4. CREW ERROR

RE-MISSION CAUSES

1. INADEQUATE EQUIPMENT DESIGN - DOES NOT MEET PERFORMANCE OR RELIABILITY REQUIREMENTS IN KNOWN OR PREDICTABLE MISSION ENVIRONMENT(S).
2. INADEQUATE MISSION PLANNING AND PROCEDURES.
3. INADEQUATE PROTECTION AGAINST DAMAGING OR INJURIOUS INTERACTIONS BETWEEN EQUIPMENT AND CREW.
4. CREW OVERSTRESSED.
5. IMPROPER OR INADEQUATE MANUFACTURING, HANDLING, TESTING OR INSPECTION.
6. INADEQUATE SELECTION AND TRAINING OF PERSONNEL.

ROPAGATION

1. NONE - IMPAIRMENT CONTAINED.
2. INTERNALLY GENERATED STRESSES THAT PROGRESSIVELY IMPAIR THE EQUIPMENT.
3. EXTERNALLY IMPOSED STRESSES THAT PROGRESSIVELY IMPAIR THE EQUIPMENT.
4. INTERNALLY GENERATED STRESSES THAT PROGRESSIVELY IMPAIR THE CREW.
5. EXTERNALLY IMPOSED STRESSES THAT PROGRESSIVELY IMPAIR THE CREW.

REW AND EQUIPMENT STATUS

CREW	EQUIPMENT
A. UNIMPAIRED	1. UNIMPAIRED
B. IMPAIRED	2. MINOR DEGRADATION
C. INCAPACITATED	3. MAJOR DEGRADATION
	4. INOPERATIVE

ISSION IMPACT

1. CONTINUE MISSION
2. MODIFY MISSION
3. ABORT MISSION
4. ESCAPE OR AWAIT RESCUE
5. NO OPTIONS

ND RESULT

REW	MISSION OBJECTIVE(S)
SAFE	1. ACCOMPLISHED
SAFETY COMPROMISED	2. PARTIALLY ACCOMPLISHED
LOST	3. NOT ACCOMPLISHED

Figure 4.4

Bendix Aerospace Systems Division

SYSTEM SAFETY RECORD SHEET

Date _____ Pag _____

Program _____

System _____

Phase _____

SUBSYSTEM/TASK	SAFETY CONSIDERATION	HAZARD POTENTIAL	TECHNICAL APPROACH OR SOLUTION	CONTROL POINTS

Figure 4.5

4.3 HAZARD REDUCTION

The recommendation for reduction of hazards identified in the course of this system safety program shall be in the following order of precedence:

4.3.1 Design for Minimum Hazard

The major effort throughout the design phases shall be to insure inherent safety through the selection of appropriate design features.

4.3.2 Safety Devices

Known hazards which cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem or equipment.

4.3.3 Warning Devices

Where it is not possible to preclude the existence or occurence of a known hazard, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application shall be designed to minimize the probability of wrong signals or improper personnel reaction to the signals.

4.3.4 Special Procedures

Where it is not possible to reduce the magnitude of an existing or potential hazard through design, or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of safety. Precautionary notations shall be standardized in accordance with established operating procedures.

4.3.5 Residual Hazards

Hazards for which safety or warning devices and special procedures cannot be developed shall be specifically identified as residual hazards. A continued effort to eliminate or reduce these hazards shall be accomplished throughout the program by maintaining awareness of new safety technology or devices being developed and their application to the experiment. Justification for the retention of residual hazards shall be documented in the final detailed hazard analysis report.

4.4 REPORTING

Reporting shall be accomplished within this plan per the System Safety Report Schedule, Figure 4.6.

4.4.1 Hazard Analysis Reports

The results of the hazard analysis described in detail in paragraphs 4.2.1 thru 4.2.2 shall be submitted as formal reports per the schedule in Figure 4.6.

4.4.2 Safety Assessment Reports

Safety assessments follow a format of Figure 4-7 and are keyed to major milestone reviews. They contain a summary statement of all safety activity since the previous milestone review and emphasize current status of hazard analysis in progress, hazard reduction activities and a listing of anticipated residual hazards.

4.4.3 Accident/Incident Report

The Accident/Incident Report (Figure 4.8) is used to document accidents and incidents along with the pertinent details of the particular occurrence and appropriate recommendations for preventive measures and corrective action. The objective of this report is to:

- ensure a thorough investigation of all accident/incident occurrences which occur within the program which may indicate the necessity of a design or procedural change.
- determine the primary and contributing causes of each occurrence.
- identify and disseminate a corrective action which may prevent recurrence of similar accidents or incidents.

Reports shall be submitted only on those accidents or incidents which can be reasonably related to a unique condition existing in the hardware or other activities related to this contract and which affect the design or operation of end items. Unrelated, routine industrial accidents in which the corrective action does not affect the design or operation of end items will not be reported. The necessity is recognized to report pertinent "near misses" which do not result in injury or damage in a particular instance, but which are indicative of an inherent hazard requiring corrective action.

4.4.4 Submittal of Reports

System Safety reports submitted to the Contracting Officer shall be directed to the attention of MSC Program Management Safety Office, Experiments, SN, or as otherwise directed.

SYSTEM SAFETY REPORT SCHEDULE

TITLE	TYPE	SUBMITTAL
Safety Assessment, PDR, FTR	II	At Meetings
Gross Hazard Analysis & Assessment	II	PDR
Crew/Mission Operations Hazard Analysis	II	CARR
Accident/Incident Reports	II	As Required

Figure 4.6

STANDARD OUTLINE
SYSTEM SAFETY PROGRESS REPORT

SUBJECT: System Safety Progress Report
Program:
Contract:
Report Period:

1. Identified Hazards
   - Description
   - Status
   - Disposition*

2. Design Changes Affecting Safety
   - Description (report at highest level appropriate; i.e., ECP package preferable to individual drawings)
   - Status
   - Disposition*

3. Identified Safety Discrepancies
   - Description (facility, procedure, waivers and deviations, etc.)
   - Status
   - Disposition*

4. Test and Operational Procedures
   - Number identified_____
   - Number reviewed_____
   - Number containing hazardous sequences_____
   - Description of hazardous sequences identified since previous report

5. System Safety Documents Submitted Since Previous Report
   - Identification
   - Title
   - Date
   - Abstract, if appropriate

6. Residual Hazard List

7. Narrative (as appropriate)

*Drop after reporting final disposition.

Figure 4.7

Bendix Aerospace Systems Division

ACCIDENT/INCIDENT REPORT

SYSTEM SAFTY ENGINEERING

TO:	1) DATE	2) REPORT NUMBER
	3) TIME	4) PROGRAM
	5) LOCATION	6) TYPE OF OCCURRENCE
	7) LOSS OF WORK/TEST TIME (ESTIMATED MAN-HOURS	8) IMPACT ON SCHEDULE

9) DESCRIBE OCCURRENCE AND IDENTIFY CAUSE FACTORS

10) EQUIPMENT AND/OR FACILITIES INVOLVED (INCLUDING COMMENT ON SAFETY EQUIPMENT)

11) EXTENT OF DAMAGE TO EQUIPMENT AND/OR FACILITIES (ESTIMATE)

12) INJURIES SUSTAINED BY PERSONNEL	13) DEFICIENCIES NOTED IN EMERGENCY EQUIPMENT/PROCEDURES

14) PREVENTIVE MEASURES AGAINST RECURRENCE AND RECOMMENDATIONS FOR PERMANENT CORRECTIVE ACTION

15) HOW DOES THIS ACCIDENT INCIDENT AFFECT THE DESIGN OR OPERATION OF A DELIVERABLE END ITEM?

PROJECT ENGINEER	SYSTEM SAFETY ENGINEER	PROGRAM MANAGER

970 78

FIGURE 4.8