~~SECRET~~/

BIF003W/B-236351-84
REV. A

25X1

Sheet Count: 25 24
Copy No: X 24
Unit 10

7 MAR 1984

FINAL

LORRI II
SYSTEM SAFETY PROGRAM PLAN

[redacted]

25X1

Prepared:

[redacted]

[redacted]

CLASSIFIED BY: BYE-1
REVIEW ON: OADR

WARNING - THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION.

0388A

~~SECRET~~/

[redacted]

Handle Via BYEMAN
Control System Only

25X1

25X1

FOREWORD

This document has been prepared in accordance with the requirements of Sequence No. A004 to contract [redacted]

25X1

25X1

TABLE OF CONTENTS

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

LIST OF ILLUSTRATIONS

LIST OF TABLES

ACRONYMS

AGE	Aerospace Ground Equipment
CCN	Contract Change Notice
CDR	Critical Design Review
CSE	Chief System Engineer
MSE	Manager SCD System Engineer
OPS	Program Operations
PDR	Preliminary Design Review
PM	Program Manager
PSA	Preliminary Safety Analyses
PSEE	Program System Effectiveness Engineer
PSSC	Program System Safety Committee
RZE	Responsible Equipment Engineer
SEE	Program System Effectiveness
SSE	System Safety Engineer
SSP	System Safety Plan
SSPP	System Safety Program Plan

HANDLE VIA BYEMAN CONTROL SYSTEM ONLY

Section 1

INTRODUCTION

This plan describes the System Safety Program (SSP) that will be implemented during the design, development, manufacture, test, and operational phases of the LORRI II program. This plan provides a disciplined approach to the identification and control of hazards. It lists the requirements, delineates the responsibilities, and describes the procedures and methods that will integrate system safety into the program.

If the analysis described herein results in a determination of safety impact on or by other than new equipment, a CCN will be generated to cover the necessary corrective action.

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

Section 2

APPLICABLE DOCUMENTS

The following documents apply to the extent specified herein:

Government Documents

MIL-STD-1574A	Systems Safety Program for Space and Missile Systems
SAMSOR 127-8	System Safety Engineering, 11 Sept 1978
SAMSO Pamphlet 127-5	SAMSO Standard Satellite System Safety Design Criteria, 1 Mar 1973

Contractor Documents

SSD-PD-P-82	SSD Safety Programs
E-400	Test Aids and Auxilliary Test Equipment
MPD 1.15 Rev 3	Safety of Products and Services
MPD 1.16 Rev 4	Accidents, Incidents, and Significant Events Involving Products and Services
C-12	Safety and Industrial Hygiene Standards

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

Section 3

SAFETY PROGRAM MANAGEMENT

3.1 ORGANIZATION AND RESPONSIBILITES

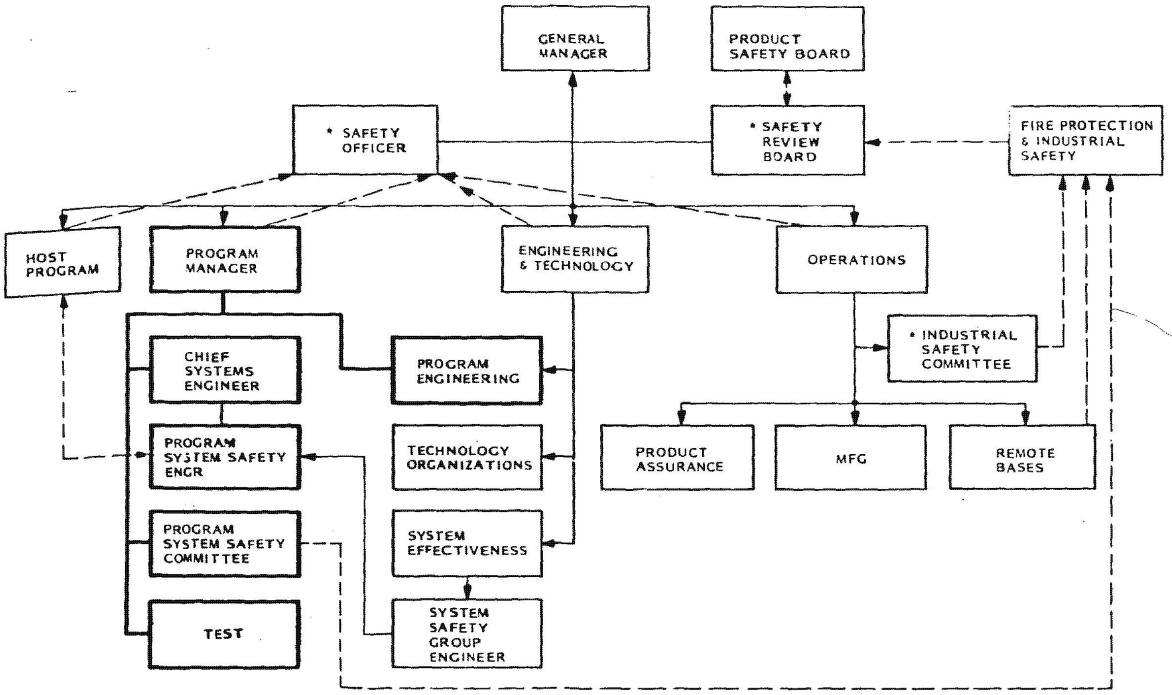
The LORRI II Program Manager is responsible for program system safety. The Contractor System Effectiveness organization (Fig. 3-1) is responsible to ensure adequate support for reliability, maintainability, and program system safety on all SSD programs.

A System Saftey Engineer (SSE) within the Contractor System Effectiveness organization will be assigned the responsibility for system safety activities specified in this plan. The System Safety Engineer will be responsible for planning, implementing, coordinating, and controlling the LORRI II system safety tasks described herein.

3.2 PROGRAM SAFETY COMMITTEE

The LORRI II Program System Safety Committee (PSSC) will assure that adequate safety standards and requirements are met in the LORRI II Program. Each committee member will function in a dual capacity, i.e., as a PSSC member and in his regular assignment. The chairman of the PSSC will be the program System Safety Engineer appointed in accordance with Policy Directive P-82.

PSSC membership will consist of appointees from the following areas as determined necessary by the chairman: (1) Program Office, (2) Manufacturing and Test Operations, (3) Host Vehicle Operations, (4) Product Assurance, (5) Program Engineering, and (6) System Effectiveness. Industrial Safety and Hygiene will participate in an advisory capacity. The committee will review and analyze product designs and test procedures associated with hazardous conditions, as well as hazardous systems and operations, in order to assure that optimum system safety has been incorporated into program products. Follow-up and closure of LORRI II PSSC action items is the responsibility of the chairman, using the System Safety Hazard Report described in Section 8 of this plan.



*SAFETY OFFICER IS CHAIRMAN OF SAFETY REVIEW BOARD AND MEMBER OF INDUSTRIAL SAFETY COMMITTEE PER POLICY DIRECTIVE P-82.

Fig. 3-1 Contractor Systems Effectiveness Organization

25X1

3.3 SAFETY REVIEW BOARD

In addition to the foregoing management and technical alignment, LORRI II system safety is independently monitored and evaluated by the Safety Review Board. This board is the highest safety level within the Contractor organization. The Safety Review Board will convene periodically to review the safety aspects of the LORRI II Program.

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

Section 4

SYSTEM SAFETY PROGRAM TASKS

The system safety tasks described in various sections of this plan are shown in Table 4-1. These tasks will be performed and checked as indicated in Table 4-2. A schedule for completing all work will be developed by the PSSC and included in the safety plan.

Table 4-1

SYSTEM SAFETY TASKS

Task	SSPP Paragraph No.	Action Responsibility
System Safety Program Plan	N/A	SSE, MSE, PM, CSE
Review change documents	10.4	SSE, REE
Request safety tests	10.2	SSE
Utilize hazard data from customer and interfacing contractors	7.1	SSE
Support development of safety criteria	3.2, 10.1, 5.3	SSE,
Preliminary Hazard Analysis	5.1	SSE, CSE
Subsystem Safety Analysis	6.1, 6.3, 4,	SSE, CSE, REE
Operating Hazard Analysis of committee-approved elements	6.2, 6.3, 4, 8, 9	SSE, CSE, OPS
Design Review Participation	4, 6.2	SSE

Responsibility Abbreviations:

SSE - System Safety Engineer
MSE - Manager SSD System Effectiveness
PM - Program Manager
CSE - Program Chief Systems Engineer
REE - Responsible Equipment Engineer
OPS - Program Operations

Table 4-2

PERFORMANCE OF SYSTEM SAFETY TASKS

Function	Milestone - Program Event When Data Developed By Function is Reviewed	Data To Be Reviewed
Preliminary Hazard Analysis	Preliminary Design Review (PDR)	1. Identification of safety critical program aspects. 2. Design criteria developed. 3. Safety critical item specifications. Completed system safety criteria. 4. Host vehicle safety criteria utilization.
Operating Hazard Analysis (Prelim)	Final Design Review (Flight Readiness)	1. Safety critical aspects of events, operations systems facilities and processes. 2. Analysis of safety critical system operation or event showing how and when hazards can occur. 3. Operational action required to minimize occurrence. 4. Identification of procedural sequence which contains hazard potential. 5. Identification of warning and caution notes to be used prior to critical procedural step.
Operating Hazards Analysis (Final)	120 Days Prior to Beginning Initial Operations	1. Completed action item list. 2. Prerequisite testing requirements data to be reviewed. 3. Emergency equipment requirements. 4. Ground handling, storage, and transportation safety requirements. 5. Emergency procedures. 6. Safety training requirements. 7. Procedural controls.

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

Section 5

SYSTEM SAFETY CRITERIA

5.1 HAZARD EVALUATION

Hazards will be classified as acceptable or unacceptable. The acceptability of a hazard is determined by the consequences of adverse effects of the hazard, the probability of occurrence of the adverse effects, the consequence on mission performance of eliminating the hazard (or the gain realized by accepting the presence of the hazard), and the cost of eliminating the hazard while maintaining required mission performance.

Consequences to be considered are impact on mission, cost of replacing damaged equipment, and schedule delays.

Acceptable hazards are those having non-serious consequences and those having low probability of occurrence combined with more serious consequences. Corrective action is required for all hazards judged unacceptable on any stage in the review. The order of precedence is defined in Section 5.2.

5.2 SYSTEM SAFETY PRECEDENCE

Actions for satisfying safety requirements in order of precedence are:

a. Design for Acceptable Hazard. The major effort throughout the program shall be to select appropriate safety design features.

b. Safety and Protection Devices. Hazards which cannot be eliminated through design selection, or which are discovered too late for basic system redesign, will be reduced to an acceptable level through the use of appropriate safety devices or protective systems consistent with program goals and objectives.

c. Warning Devices. Where it is not possible to preclude a hazard, reliable warning devices with proper emergency plans will be employed for timely detection of the likelihood or imminence of an accident and the generation of an adequate warning signal. Warning signals will be used and standardized where appropriate to minimize the probability of improper personnel reaction to the signal(s). Personnel will be properly trained with regard to the purpose of the warning device(s) and what to do when signals occur.

d. Special Procedures. Where it is not possible to reduce the magnitude of hazards through design change, appropriate emergency procedures will be developed. Personnel will be properly trained regarding the use of these procedures.

5.3 SAFETY DESIGN CRITERIA

LORRI II Program safety design criteria will be established in accordance with guidelines and standard design practices provided in the Contractor design handbooks and in SAMSO pamphlet 127-5, and will be provided to designers for use. New equipment will be designed to eliminate, minimize, or control hazards through the incorporation of these safety design criteria as appropriate.

Section 6

SYSTEM SAFETY ANALYSES

The types of system safety analyses to be performed for the LORRI II Program are described in the following sections. The system safety analyses will proceed as shown in the flow diagram of Fig. 6-1. The result of this assessment will be a definition of those factors and conditions that will be considered hazardous throughout the program. Corrective measures to eliminate or control identified hazards will be recommended. This definition provides a program baseline for formulation of design criteria and assessment of the adequacy of existing systems analyses, operation plans, and operations analyses. These criteria, in addition to hazard analysis results, will also be used in the system safety input to design reviews.

6.1 PRELIMINARY HAZARD ANALYSIS

The qualitative preliminary hazard analysis will provide the initial assessment of system safety aspects for the LORRI II Program as related to new equipment. The safety impact on the existing system, facility, end item, event, operation, or process will also be evaluated with regard to safety criticality. This analysis will be conducted by the System Safety Engineer (SSE), under the direction of the CSE.

6.2 OPERATING HAZARD ANALYSIS

Safety operating requirements for safety-critical aspects determined by the preliminary and subsystem hazard study will be identified.

Prerequisite testing requirements for safety-critical items such as lifting or handling equipment and ordnance or propulsive devices, are included.

Identification of emergency equipment and its location will be selected for each identified critical event or operation and will be included in the appropriate procedure.

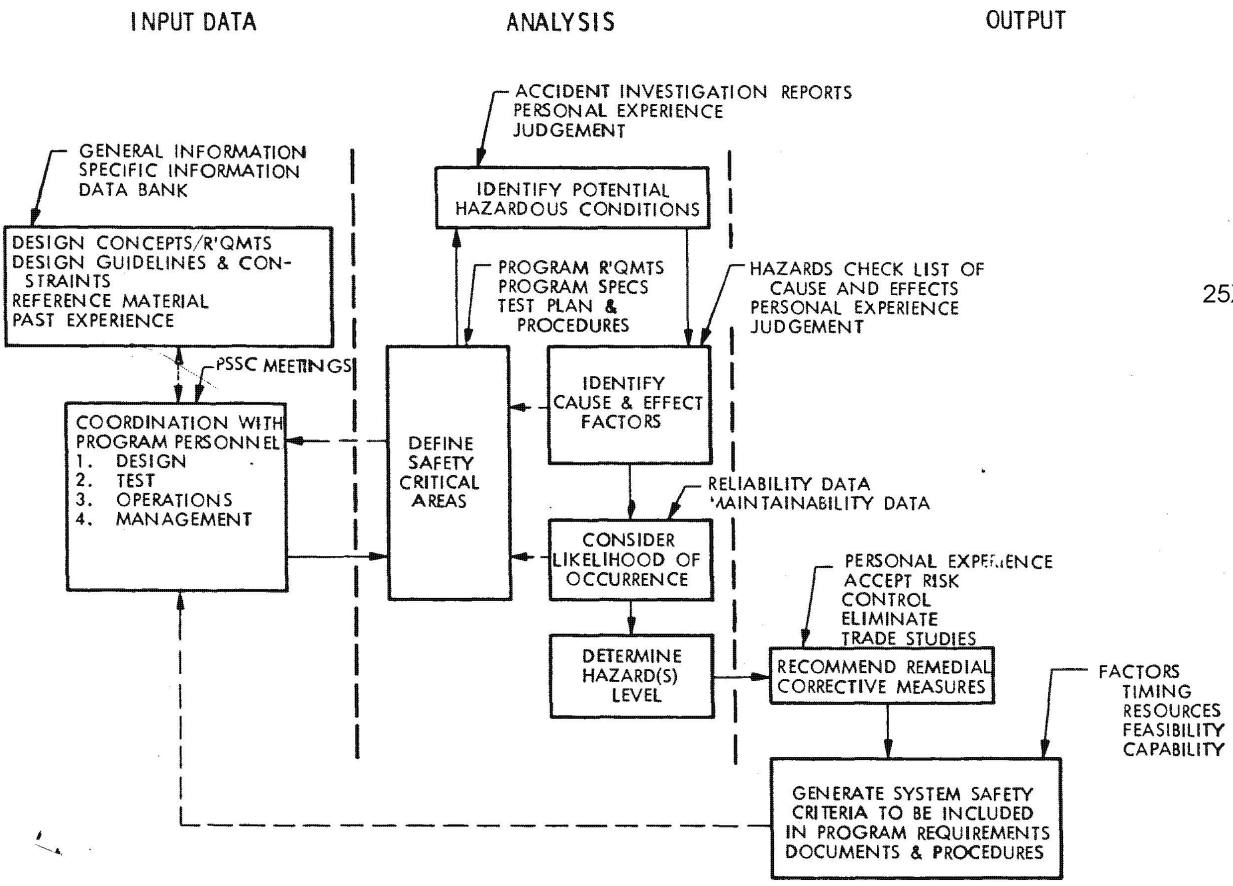


Fig. 6-1 Program System Safety Analysis Flow Diagram

25X1

The safety requirements and restrictions resulting from this analysis will be used as inputs to test procedures. These requirements and restrictions will be brought to the attention of those responsible for test plans and procedures through several means. They will be identified in hazard analysis reports, and/or in system safety hazard reports (see Section 8), and in design reviews. Finally, as a check on all of these means, system test procedures are reviewed by Program System Effectiveness.

In addition, this analysis will produce information suitable for submittal to the host vehicle program for approval in accordance with the appropriate host vehicle manual. Preliminary results of this analysis will be presented at the critical and final design reviews (flight readiness) and where necessary, corrective action measures will be delineated.

6.3 POSTANALYSIS ACTIONS

Hazards identified during the system safety analyses will be brought to the attention of the organization responsible for the equipment or activity involved. In cases where interfaces are involved, the system engineering organization will participate. The Program System Safety Engineer will participate in determining corrective action and in deciding if the corrective action is adequate to preclude the hazard.

When hazardous conditions are identified which cannot be eliminated, the customer will be notified.

Section 7

SAFETY ACTIVITIES

7.1 SAFETY DATA

A file of safety data and correspondence prepared by the Contractor in fulfillment of the system's safety effort will be maintained and made available to the contracting officer, when required, for the duration of the contract period.

Utilization will be made of safety data from other associate or subcontractors, and other Government or industry sources.

7.2 TRAINING

Inputs will be made to the training courses for operating personnel when it is determined that new and modified equipment has created hazardous conditions affecting such training.

Section 8

AUDIT PROGRAM

The following documents will be audited for safety considerations:

a. Engineering drawings: GSE and end items
b. Safety reports (preliminary hazard analysis)
c. Handling procedures
d. Test setups

Recommendations will be made for assignment of responsibility for resolution of safety action items and follow-up on safety items assigned to assure satisfactory closure by use of the System Safety Hazard Report (Fig. 8-1).

In addition to internal audits, the Safety Engineer will support external audits authorized by the purchasing office. This will include independent verification and validation efforts by the Space Segment integrating contractor.

Subcontractors will be audited by the Responsible Equipment Engineer or Reliability Engineer to ensure that safety requirements are being satisfied and safety data produced to meet schedule needs.

HAZARD REPORT

NO.__REV.__

PAYLOAD	HAZARD STATUS
SUBSYSTEM	DATE
OPERATION/PHASE	CLOSURE LEAD
HAZARD/UNDESIRED EVENT	HAZARD LEVEL
	HAZARD GROUP

CAUSAL FACTORS/ASSUMPTIONS & EFFECTS

APPLICABLE REQUIREMENTS

HAZARD CONTROLS/VERIFICATION METHODS	STATUS	REFERENCE

REMARKS

CLOSURE CONCURRENCE

PROGRAM SAFETY ENGINEER	DATE	SRT CHAIRMAN	DATE
PROGRAM MANAGER	DATE	CLOSURE LEAD	DATE

PAGE__OF__

Fig. 8-1 System Safety Hazard Report

Section 9

HANDLING, TRANSPORTATION AND STORAGE

Safe ground handling and transportation equipment, facilities, and procedures are provided by the following:

a. Use of existing or slightly modified equipment by experienced personnel using existing or modified procedures.

b. For the new system equipment, the handling concepts will be established by Systems Engineering and concurred with by the SSE. The resulting procedures will be reviewed and approved by Systems Engineering and the SSE.

c. Critical handling operations will be monitored by System Safety Engineering.

d. Storage and servicing will be in accordance with procedures reviewed and approved by System Safety Engineering to assure safe conditions.

Section 10

OTHER SYSTEM SAFETY MATTERS

10.1 EXPLOSIVE AND ORDNANCE

The safety design criteria for explosives and ordnance will be provided during the safety analysis task and will be provided to designers for use as applicable for new equipment.

10.2 IN-PLANT TESTING

The in-plant testing program (development, qualification, and acceptance) will be configured so that:

a. All fixtures used to test and/or handle flight hardware shall be subject to aerospace ground equipment (AGE) controls (Ref E-400), and appropriate safety standards in manual C-12.

b. The specified corrective actions defined by the safety analysis effort are verified during the testing effort.

c. Safety and human factor requirements that are intended to minimize the possiblity of personnel error resulting in or contributing to equipment damage are included in test plans.

d. Failures are reported to the program CSE for determination of safety implications.

10.3 SYSTEM INSTALLATION

The effect of new equipment on the safety aspects of system installation will be identified during the Preliminary Safety Analyses (PSA). Required warning and safety precaution information will be developed for incorporation in appropriate procedures.

10.4 DESIGN CHANGE CONTROL

Once a design has been analyzed from a system safety standpoint and it becomes necessary to change the design, the change will be reviewed for system safety considerations by the program CSE. If the system safety review determines that the change will create a new hazard, or make an existing hazard worse, the design change package will be resubmitted to the designer together with written documentation explaining why the change is unacceptable to system safety. If the matter cannot be settled between the safety and design organizations, it will be submitted to higher authority.

10.5 MISHAP INVESTIGATION

Accidents, incidents, and failures with safety implications will be investigated in accordance with the latest revision Contractor Management Policy Directives listed below:

a. MPD 1.15 Rev 3, Safety of Product and Services
b. MPD 1.16 Rev 4, Accidents, Incidents, and Significant Events Involving Products and Services
c. SSD-PD-P-82, Safety Programs

10.6 RANGE SAFETY

Preliminary, subsystem, and operating hazard and safety analysis results will be provided to the host vehicle for incorporation into the missile system ground safety approval package for submittal to SAMTO/SE for approval prior to launch.