SOR-71-002
MARCH 1971

Prepared for
NASA Manned Spacecraft Center
under Contract NAS9-11528
DRL 30, DRD SA-019T

SYSTEM SAFETY PLAN
FOR THE
ULTRAVIOLET SPECTROMETER EXPERIMENT S169

THE JOHNS HOPKINS UNIVERSITY ▪ APPLIED PHYSICS LABORATORY

CR-128570

SOR-71-002
March 1971

SYSTEM SAFETY PLAN

FOR THE

ULTRAVIOLET SPECTROMETER EXPERIMENT S169

Prepared for
NASA Manned Spacecraft Center
Under Contract NAS9-11528
DRL 30, DRD SA-019T

Prepared by: R. G. Heidelbach
Safety Engineer

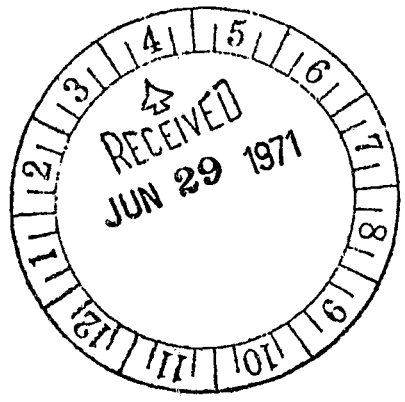
Approved by: T. Wyatt
Project Engineer

Approved by: R. W. Cole 3/24/71
R. W. Cole
Group Supervisor,
Satellite Reliability Control

Date: 26 March 71

The Johns Hopkins University
Applied Physics Laboratory
8621 Georgia Avenue
Silver Spring, Maryland

CHANGE NO. 1
JUNE 1971
SOR-71-002



MSC CONTRACT NAS9-11528
DRL 30, DRD SA-019T

SYSTEM SAFETY PLAN

FOR THE

ULTRAVIOLET SPECTROMETER EXPERIMENT S169

THIS CHANGE NUMBER ONE IS SUBMITTED TO AMEND THE ORIGINAL OF THE SYSTEM SAFETY PLAN FOR THE ULTRAVIOLET SPECTROMETER EXPERIMENT S169. INSTRUCTIONS FOR INCORPORATING THIS CHANGE INTO THE PLAN ARE AS FOLLOWS:

1. Insert this new page into the plan, following the present sign-off title page.

2. Insert the accompanying new "List of Effective Pages" into the plan following this page.

3. Replace the present Pages 1, 2, 5 and 7 with the new pages of the same numbers.

PREPARED BY: R. G. Heidelbach
R. G. Heidelbach
Safety Engineer

APPROVED BY: T. Wyatt
T. Wyatt
Project Engineer

DATE: 22 June 1971

APPROVED BY: R. W. Cole for
R. W. Cole
Group Supervisor,
Satellite Reliability Control

The Johns Hopkins University
Applied Physics Laboratory
8621 Georgia Avenue
Silver Spring, Maryland

LIST OF EFFECTIVE PAGES

PAGE NUMBER	CHANGE NUMBER
i	Original
ii	Original
iii	Original
1	One
2	One
3	Original
4	Original
5	One
6	Original
7	One
8	Original
9	Original
10	Original
11	Original
12	Original
13	Original

NOTE: ON CHANGED PAGES, THE AFFECTED AREA IS INDICATED BY A VERTICAL LINE IN THE RIGHT-HAND MARGIN ALONGSIDE THE AFFECTED AREA.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

LIST OF ILLUSTRATIONS

1.0 SCOPE

1.1 PURPOSE

The purpose of this document is to define comprehensive safety program requirements, and present a methodology for implementing the defined safety tasks in support of the design, development, manufacturing, testing and flight phases of the Ultraviolet Spectrometer Experiment S169.

1.2 OBJECTIVE

The objective of this plan is to identify all critical or catastrophic type hazard areas, and to seek to totally eliminate such hazards wherever possible, or seek to minimize the occurrence and/or the effects of those hazards that cannot be totally eliminated.

This plan is applicable to all elements of the APL role as contractor for this experiment. As such, this plan covers all safety aspects relating to hardware, software, ground support equipment (GSE), Government Furnished Equipment (GFE), and to all associated activities pertaining to design, manufacture, checkout, test training, handling, transportation and storage of the ultraviolet spectrometer equipment.

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents form a part of this plan to the extent specified herein:

MSCM 1701, "System Safety Plan (Manned Space Flight Program)"

MSCI 8825.3, "MSC Test Safety Review Committee"

MSCI 8825.2, "Operational Readiness Inspections of Facilities and Equipment Involving Man in a Vacuum or Oxygen-Rich Environment"

MSCI 8825.1A, "Operational Readiness Inspections of MSC Test Facilities and Equipment"

MSCM 1700, "MSC Safety Manual, Part 7 - Man Rating Requirements"

MSC Directive of January 1969, "System Safety Requirements for Manned Space Flight"

3.0 DEFINITIONS

3.1 SAFETY TERMS

a. Safety - Freedom from chance of injury or loss to personnel, equipment or property.

b. System Safety - The organized application of scientific and engineering techniques and analyses for the identification of potential hazards throughout all phases of the program life cycle.

c. Public Safety - The extension of system and industrial safety for the protection of the general public.

d. Hazard - Condition(s) which can cause personnel injury or death, significant loss of equipment or property, and/or produce harmful change in the natural earth environment.

e. Inherent Hazard - The presence of a risk resulting from equipment design, equipment intrinsic nature, environment, procedural deficiency, or combinations of these conditions.

3.2 HAZARD CATEGORIES

Hazard categories are established to assure that potentially hazardous systems or associated crew procedures, identified by the hazard analysis, receive proper attention in the design phase. These systems and/or procedures will be placed in the appropriate hazard category:

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

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

c. Safety Marginal - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or sub-system failure or component malfunction

will degrade system performance but which can be counteracted or controlled without major damage or any injury to personnel.

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

4.0 MANAGEMENT

4.1 POLICY

The APL System Safety Program provides for an organized activity in which management efforts and technical disciplines are coordinated to provide timely identification and the required corrective action to eliminate or control those conditions or events that will contribute to injury or loss of crew, operating personnel, system failure, or damage to equipment and hardware throughout all phases of the program.

4.2 MANAGEMENT AND CONTROL

Management and control policy provides for and insures implementation of the following:

a. Specialized safety engineering and technical competency for system safety and crew safety tasks.

b. Functional participation by "in-line" disciplines in the safety program effort.

c. Management awareness of risks and requirements for risk management.

d. Establishment and compliance with safety requirements and criteria that are commensurate with the scope of the Apollo Program.

4.3 ORGANIZATION

The APL Safety Organization for the Ultraviolet Spectrometer Experiment has been structured as shown in Figure 1. The Safety Engineer is the single focal point for the total safety program management and responsibility. He will establish direct contact with the Project Engineer, when required, concerning safety requirements and safety problems.

5.0 SYSTEM SAFETY TASKS

5.1 GENERAL

The system safety plan for this experiment is described, and the general requirements and associated safety tasks to be performed by APL are outlined in the following paragraphs.

5.1.1 Reports and Documentation Files

5.1.1.1 Monthly Safety Progress Reports - Monthly Safety Progress Reports will be submitted to MSC as a part of the Monthly Program Progress Report and will contain:

a. Status of safety reviews conducted and those procedures or items identified as "Safety Critical".

b. Hazards identified as Critical or Catastrophic with disposition of the action requirements and status of corrective action.

c. Design changes affecting safety and their status.

d. Safety discrepancies, their disposition, and status.

e. Summaries of accident/incident and failure reports, as necessary.

5.1.1.2 Formal safety assessments will be submitted two weeks prior to the Critical Design Review.

5.1.1.3 System Safety significant activities or critical safety problems will be reported as soon as possible upon identification.

5.1.1.4 APL will establish a safety file as a central control point for all documentation relating to the safety program. This file will include but not be limited to:

Correspondence
Safety Plans
Directives
Engineering System Safety Analyses
Operations System Safety Analyses
Safety Manuals
Hazardous Materials Controls

Waivers/Deviations
Reports to MSC
Audit Reports
Accident/Incident File
Safety Corrective Action File
Safety Alerts

5.1.2 Reviews

The Safety Engineer will participate in reviews for assessment and resolution of safety problems and insure response to MSC identified hazards.

5.1.3 Audits

Existing design drawings will be reviewed for safety consideration of mechanical design, i.e., sharp edges and protuberances, burrs, improper arrangement, pinch points and shear points. Electrical design will be reviewed for possible electric shock hazards and necessary current limiting devices where required. All hardware will be reviewed for safety of operation in specified environments involved in flight. Special item purchase requisitions will be reviewed for safety requirements. Incoming parts inspection of vendor items will be monitored as required for safety compliance. Vendor sites will be inspected during fabrication of those parts which may not be capable of being checked after assembly. Vendor item specifications will be reviewed for compliance with safety requirements. In-house fabrication processes will be monitored to insure safety

5.1.6 Safety Waivers and Deviations

Safety Waivers and Safety Deviations will be submitted to MSC for concurrence.

5.1.7 NASA Alerts and Technical Information Bulletins

NASA Alerts and Technical Information Bulletins will be reviewed for safety implications and application to this Experiment, and filed for future reference.

5.1.8 Crew/Mission Operations Safety

This paragraph describes the Crew/Mission Operations Safety tasks to be accomplished to insure the safety of the flight crew in design, interfacing systems, and the conduct of mission operations analyses.

5.1.8.1 Requirements - The APL developed safety design requirements for this Experiment will be included in applicable design drawings, specifications, and engineering requirement documents. All changes to these documents will be reviewed for compliance with system safety requirements.

5.1.8.2 Reviews - APL will support and participate in reviews including Critical Design Reviews and Acceptance Reviews to establish that system safety requirements have been satisfied and waivers and deviations have been approved.

5.1.8.3 Analyses and Studies - APL will perform the following evaluations and studies to identify all systems and experiment interface problems.

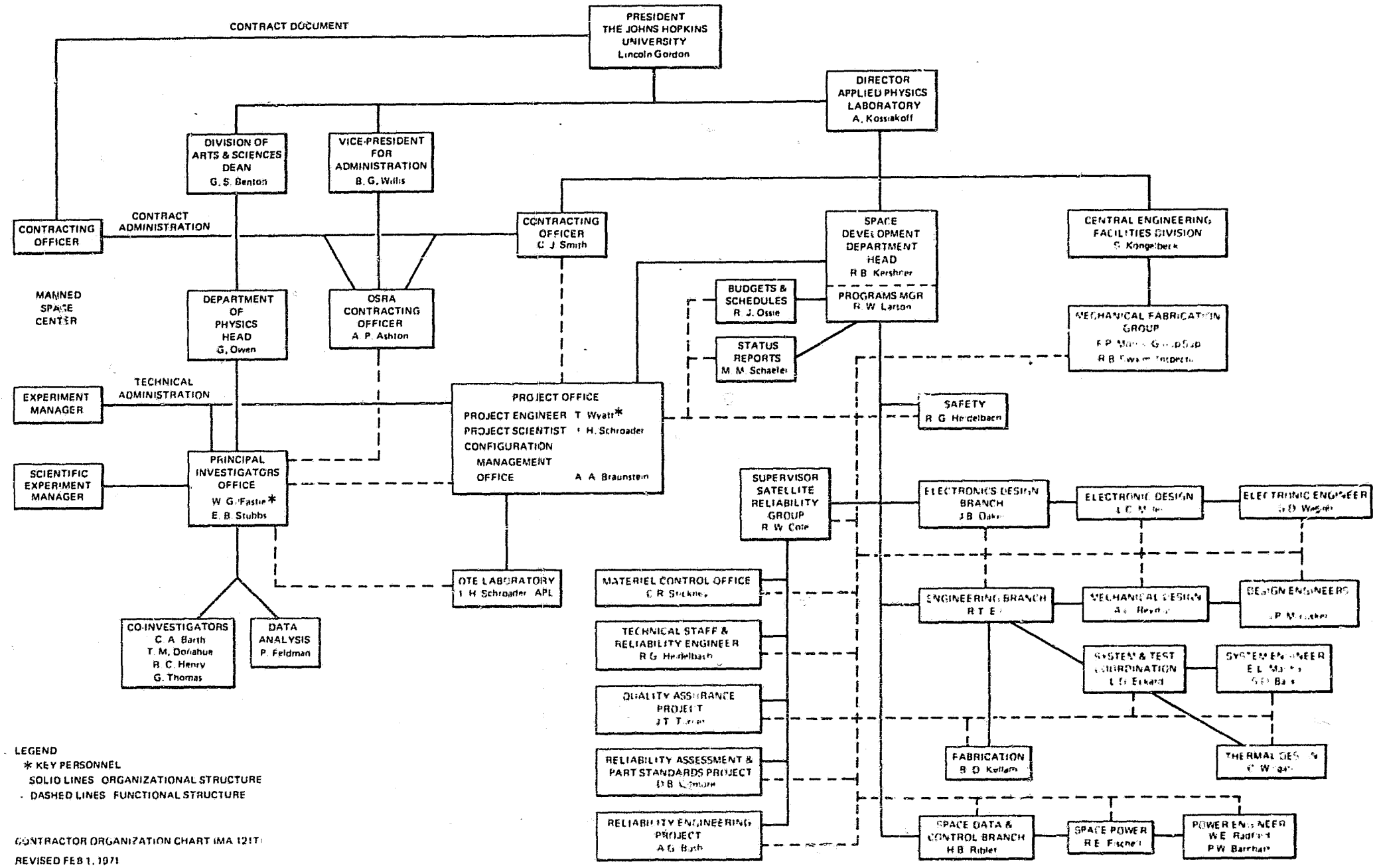
5.1.8.3.1 Overall experiment analysis will be conducted early during initial design stages on equipment and operating procedures to identify and categorize problems affecting crew safety. Identified hazards will be classed in accordance with the MSC directive of January 1969, "System Safety Requirements for Manned Space Flight".

5.1.8.3.2 Detailed system analyses using Failure Mode and Effects Analysis (FMEA) activity for each failure mode will be conducted. Analysis will determine the effects on interfacing systems to insure that problems do not propagate across the interface. Such effects will be classified in accordance with the Hazard Categories of the MSC directive of January 1969, "System Safety Requirements for Manned Space Flight".

5.1.8.3.3 Operational hazard analyses will be conducted to identify operational problems relative to the experiment and its support equipment. Analysis methodology will be to identify the function and corresponding tasks. Hazards associated with the task will be identified to establish their effect on personnel, equipment, facilities, and airborne hardware. All hazards will be categorized to identify cause, criticality, and recommended controls. Status will be maintained until all identified hazards are resolved. Operational hazard analyses will utilize all other analysis data in the selection of the operations to be covered to preclude redundancy of effort.

5.1.8.3.4 A study will be conducted of all manually initiated experiment commands to determine potential for error and the effects of such errors.

5.1.8.4 Identified Hazards - All identified hazards will be reported to the Project Engineer for resolution as outlined in the System Safety Organization flow chart of Figure 2.



LEGEND
* KEY PERSONNEL
SOLID LINES ORGANIZATIONAL STRUCTURE
DASHED LINES FUNCTIONAL STRUCTURE

CONTRACTOR ORGANIZATION CHART (MA 121T)
REVISED FEB 1, 1971

FIGURE I

SYSTEM SAFETY PLAN

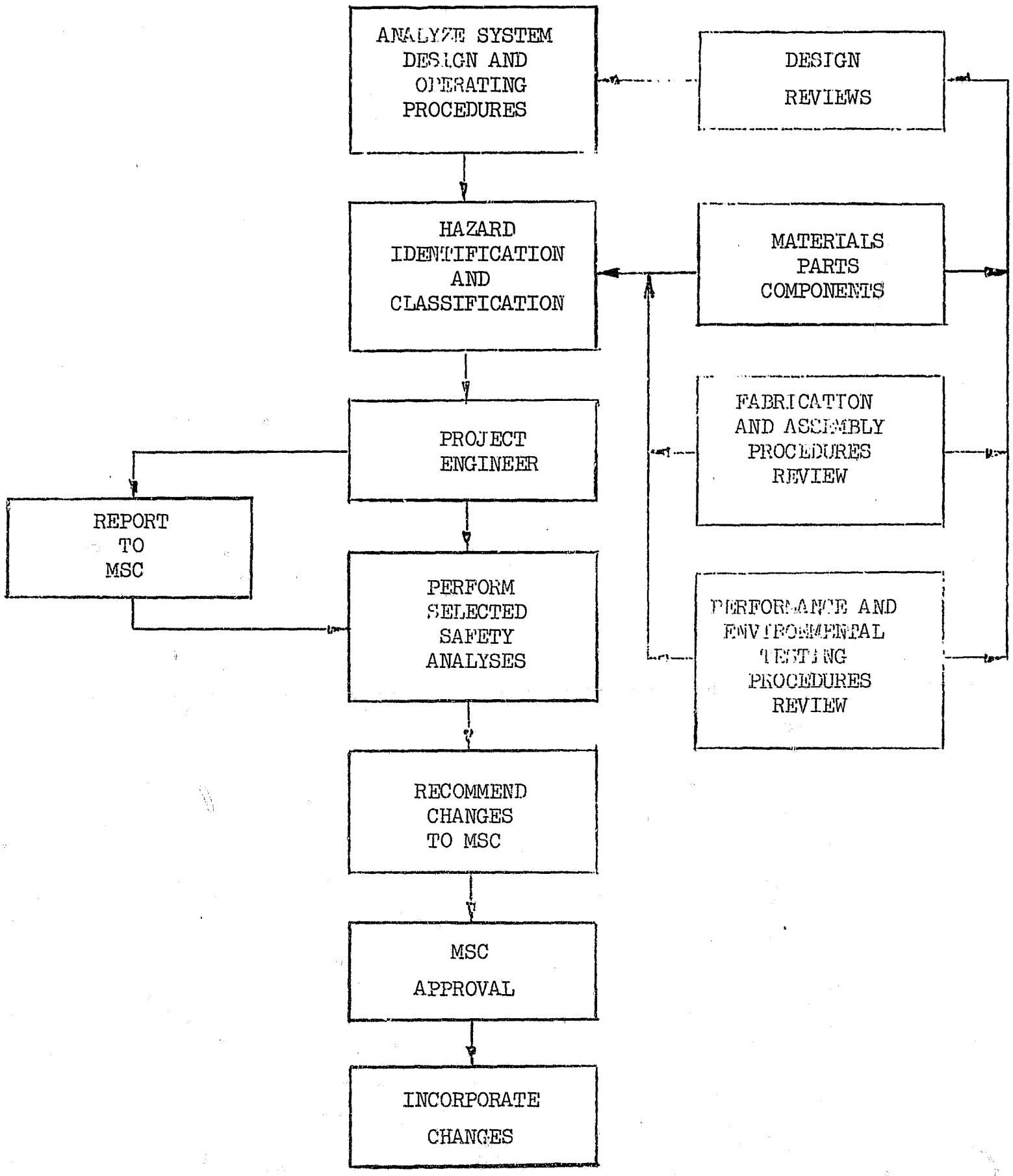


FIGURE 2