

NOT MEASUREMENT
SENSITIVE

National Aeronautics and
Space Administration

NASA-STD-8719.7
January 1998

FACILITY SYSTEM SAFETY GUIDEBOOK

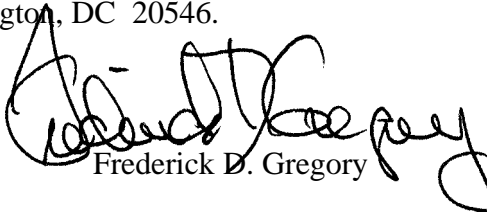
NASA TECHNICAL STANDARD

FOREWORD

Effective Date: January 30, 1998

This NASA Technical Standard (NTS) provides a guideline for NASA facility and safety professionals who are involved with the facility acquisition or modification/construction process and life cycle phases at NASA installations. This document provides fundamental information for the development of a facility safety program during the acquisition process and the framework for implementing facility system safety goals and requirements into NASA facilities. Safety is an integral aspect of the facility acquisition process and must be considered at all phases throughout the life cycle of the facility system. This document has also been developed to support the NASA Safety Training Center (NSTC), "Facility System Safety Course."

Comments regarding this document should be addressed to the Director, Safety and Risk Management Division, NASA Headquarters, Washington, DC 20546.



Frederick D. Gregory

Associate Administrator for
Safety and Mission Assurance

DISTRIBUTION:

SDL1 (SIQ)

TABLE OF CONTENTS

PARAGRAPH		PAGE
	<u>FOREWORD</u>	i
	<u>TABLE OF CONTENTS</u>	ii
	<u>APPENDICES</u>	iii
	<u>LIST OF FIGURES</u>	iv
	<u>LIST OF TABLES</u>	iv
1.	<u>SCOPE</u>	
1.1	Purpose	1-1
1.2	Applicability	1-1
1.3	Organization of Handbook	1-1
2.	<u>REFERENCED DOCUMENTS</u>	
2.1	Government Documents	2-1
2.2	Commercial Publications	2-1
2.3	Order of Precedence	2-1
3.	<u>DEFINITIONS AND ACRONYMS</u>	
3.1	System Safety Definitions	3-1
3.2	System Safety Acronyms	3-1
4.	<u>GENERAL</u>	
4.1	Introduction	4-1
4.2.	Processes	4-2
4.3	NASA Safety Policy and Requirements	4-4
5.	<u>FACILITY SYSTEM SAFETY PROCESS</u>	
5.1	Introduction	5-1
5.2	Requirements Phase	5-1
5.3	Planning Phase	5-11
5.4	Design Phase	5-24
5.5	Construction Phase	5-24
5.6	Activation Phase	5-26
5.7	Operations Phase	5-27
5.8	Disposal Phase	5-27

TABLE OF CONTENTS

(Continued)

PARAGRAPH		PAGE
6.	<u>OTHER FACILITY ACTIVITIES REQUIRING A SYSTEM SAFETY INPUT</u>	
6.1	Introduction.....	6-1
6.2	Operating Procedures	6-1
6.3	Test Activities.....	6-1
6.4	Maintenance Procedures	6-2
6.5	Facility Acceptance Plans.....	6-3
6.6	Training Plans.....	6-4
6.7	Configuration Management Plans.....	6-5
6.8	Emergency Management Plans.....	6-5
7.	<u>OTHER HAZARD ANALYSIS METHODOLOGIES</u>	
7.1	Introduction.....	7-1
7.2	Energy Trace Barrier Analysis	7-1
7.3	Hazard and Operability Study	7-5
7.4	Subsystem Hazard Analysis.....	7-8
7.5	System Hazard Analysis.....	7-9
7.6	Operating and Support Hazard Analysis.....	7-9
7.7	Fault Tree Analysis	7-12
7.8	Failure Mode And Effects Analysis	7-14
7.9	Software Hazard Analysis.....	7-14
7.10	Hazard Analysis Schedules.....	7-17

APPENDICES

APPENDIX		PAGE
A	Typical Energy Sources Checklist	A-1
B	Preliminary Hazard List Example	B-1
C	Example Facility Safety Management Plan - Table of Contents.....	C-1
D	Example Facility Hazard Analysis	D-1

LIST OF FIGURES

FIGURE	PAGE
4-1 System Safety Process	4-3
4-2 NASA Safety Document Tree.....	4-6
5-1 Facility Acquisition Milestone Activities.....	5-2
5-2 Facility Project Brief Project Document (NASA Form 1509)	5-3
5-3 Example Initiator's Safety Checklist for Procurement.....	5-4
5-4 Facility Risk Indicator (FRI) Process.....	5-8
5-5 Facility Hazard Analysis Process.....	5-16
5-6 Hazard Severity Categories.....	5-17
5-7 Hazard Probability Categories.....	5-18
5-8 Hazard Risk Index Matrix.....	5-19
5-9 Hazard Reduction Precedence.....	5-20
5-10 Facility Hazard Analysis Organization Tree.....	5-22
5-11 Facility Hazard Analysis Data Sheet.....	5-22
7-1 Energy Trace and Barrier Analysis Procedure	7-1
7-2 HAZOP Process	7-5
7-3 HAZOP Worksheet	7-7
7-4 Completed Signal System SSHA Form	7-8
7-5 Completed Tunnel Pumping System SHA Form.....	7-10
7-6 Example O&SHA Worksheet	7-12
7-7 Example Fault Tree.....	7-13
7-8 Failure Modes and Effects Analysis.....	7-15
7-9 Facility System Safety Milestone Activities	7-17

LIST OF TABLES

TABLE	PAGE
4-1 System Safety Program Plan Table of Contents.....	4-5
7-1 Energy Types and Examples for Energy Traces.....	7-3
7-2 Guide/Process Condition	7-6

CHAPTER 1: SCOPE

1.1 PURPOSE. This document is a guideline for implementing a Facility System Safety Program to meet the requirements of “NASA Safety Policy and Requirements Document,” NHB 1700.1 (V1B). The facility acquisition process information was taken from the “NASA Facility Project Implementation Handbook,” NPG 8820.2. The purpose of this Facility System Safety Guidebook is to provide a guideline for facility and safety professionals who are involved with the facility acquisition or modification/construction process and life cycle phases at NASA installations and to provide fundamental information for the development of a facility safety program during the acquisition process. This guidebook provides the framework for implementing facility system safety goals and requirements into NASA facilities. Safety is an integral aspect of the facility acquisition process and must be considered at all phases throughout the life cycle of the facility system. This document has also been developed to support the NASA Safety Training Center (NSTC), “Facility System Safety Course.”

1.2 APPLICABILITY. This document provides a guideline for implementing a facility system safety program at all NASA Centers, Field Installations, and Component Facilities. In this document, the words “Center” and “Centers” refer to all NASA Centers, Field Installations, and Component Facilities. System safety methodologies and facility acquisition activities are integrated to assure safety of the completed facility. The document is based on NASA facility system safety requirements and many government and industry guidelines for facility safety. Techniques for completing Facility Hazard Analysis are addressed in sufficient detail to provide a working knowledge and a basis for continued refinement of skills.

1.3 ORGANIZATION OF HANDBOOK. This handbook is organized in a standard fashion. Section 1 addresses Scope, Section 2, Referenced Documents, Section 3, Definitions and Acronyms, and Section 4, General. Sections 5 through 7 provide technical information and guidance material.

CHAPTER 2: REFERENCED DOCUMENTS

2.1 GOVERNMENT DOCUMENTS.

NASA DOCUMENTS.

National Aeronautics and Space Administration. (1982). "Safety and Health Handbook," NHB 2710.1. Washington, DC: U.S. Government Printing Office.

National Aeronautics and Space Administration. (1997). "Facility Project Implementation Handbook," NPG 8820.2. Washington, DC: U.S. Government Printing Office.

National Aeronautics and Space Administration. (1993). "NASA Safety Policy and Requirements Document," NHB 1700.1 (V1-B). Washington, DC: U.S. Government Printing Office.

OTHER GOVERNMENT AGENCIES.

U.S. Department of Defense. (1993). "Military Standard System Safety Program Requirements," MIL-STD 882C. Washington, DC: U.S. Government Printing Office.

U.S. Department of the Army. (1988). "Facility System Safety," EM 385-1-1. Washington DC: U.S. Government Printing Office.

U.S. Department of the Navy. (1986). "Navy System Safety Program," OPNAVINST 5100.24. Washington DC: Department of the Navy.

U.S. Department of the Navy. (1987). "Command Safety and Health Program," NAVFACINST 5100.1G. Alexandria, VA: Naval Facilities Engineering Command.

2.2 COMMERCIAL PUBLICATIONS.

Hammer, W. (1980). "Product Safety Management and Engineering." Englewood Cliffs, NJ: Prentice-Hall.

Olson, R.E. (1982). "System Safety Handbook for the Acquisition Manager." Los Angeles: Space Division, U.S. Air Force Systems Command Printing Office.

Roland, H.E., & Moriarty, B. (1990). "System Safety Engineering and Management." New York: John Wiley and Sons, Inc.

2.3 ORDER OF PRECEDENCE. Nothing in this document supersedes applicable laws or regulations unless a specific exemption has been obtained.

CHAPTER 3: DEFINITIONS AND ACRONYMS

3.1 SYSTEM SAFETY DEFINITIONS. The following definitions are used in this publication:

- Hazard: Any real or potential condition that can cause injury or death, or damage to or loss of equipment or property.
- Hazard Cause: Any item that creates or significantly contributes to the existence of a hazard.
- Hazard Effects: The potential detrimental consequences of the hazard.
- Risk: The combination of the hazard severity with the likelihood of its occurrence.

3.2 SYSTEM SAFETY ACRONYMS. The following is a comprehensive list of the acronyms used in this publication:

A&E	Architect Engineering
ACGIH	American Councils of Governmental Industrial Hygienists
ADA	Americans with Disabilities Act
ASHRAE	American Society of Heating, Refrigeration, and Air Conditioning Engineers
ASTM	American Society for Testing and Materials
CFR	Code of Federal Regulations
CoF	Construction of Facilities
ETBA	Energy Trace Barrier Analysis
FHA	Facility Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FRI	Facility Risk Indicator
FSMP	Facility Safety Management Plan
HASC	Hazard Analysis Sub Committee
HATI	Hazard Analysis Tracking Index
HAZOP	Hazard and Operability Study
HLTR	Hazard List Tracking Record
HRV	Hazard Resolution Verification
IST	Initial System Test
NFPA	National Fire Protection Act
NHB	NASA Handbook
NIOSH	National Institute of Occupational Safety and Health
NMI	NASA Management Instruction
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines

NSC	National Safety Council
NSTC	NASA Safety Training Center
NTS	NASA Technical Standard
O&SHA	Operational and Support Hazard Analysis
ORR	Operational Readiness Review
OSH	Occupational Safety and Health
OSHA	Occupational Safety and Health Agency
PER	Preliminary Engineering Report
PHL	Preliminary Hazard List
PPE	Personal Protective Equipment
RAC	Risk Assessment Classification
S-P	Severity-Probability
SHA	System Hazard Analysis
SMA	Safety and Mission Assurance
SRM&QA	Safety, Reliability, Maintainability, and Quality Assurance
SSHA	Sub System Hazard Analysis
SSPP	System Safety Program Plan
UBC	Uniform Building Code
UFAS	Uniform Federal Accessibility Standard
UFC	Uniform Fire Code
UMC	Uniform Mechanical Code

CHAPTER 4: GENERAL

4.1 INTRODUCTION

According to NASA accident/incident reports, over 50 million dollars worth of damage resulted from facility mishaps during the decade 1985 to 1995. At one Center, lightning struck and damaged the Main Electrical Power Substation; poor equipment design and operational procedure failure caused over three million dollars worth of damage. At another center, a short circuit in lighting equipment created a fire, resulting in smoke and fire damage. Single point failure in a NASA wind tunnel resulted in a catastrophic loss costing over 3 million dollars. At another Center, a cooling tower collapsed and resulted in over three million dollars worth of damage. To improve the hazard identification and elimination/control process, NASA Headquarters has developed this handbook and a facility safety course.

4.1.1. System safety is a discipline that examines the total life cycle of a system or process. System safety draws professional knowledge and specialized skills in engineering, mathematical, physical, and related scientific disciplines to specify, predict, and evaluate the safety of systems and facilities. The safety achieved in a system is dependent on the importance safety is given during the requirements, planning, design, construction, activation, operation, and disposal phases of each system and facility. Designing-in safety is a prerequisite and precursor for effective operational safety. The goal is to produce an inherently safe facility that will have the appropriate level of safety controls.

4.1.2. The System Safety Concept. "Military Standard System Safety Program Requirements," MIL-STD-882, defines system safety as "the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle."

4.1.3. The goal of system safety is to optimize safety and manage the residual risks. Because safety is "the freedom from personnel injury, damage to equipment, or loss of resources (especially mission critical resources)," there are numerous system components that the engineer must consider. The principal elements are people, equipment, facilities, environment, and the time frame. Risk management is the administration of all of these elements and optimal control of risks within the constraints of system operational effectiveness, schedule, and cost.

4.1.4. System safety is based on the approach of studying the entire system under all possible operating conditions. The total system is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirements. The system safety process is a systematic approach to safety program management, requirements identification, analysis of systems, and documentation of results throughout the entire program life cycle.

4.2. PROCESSES

4.2.1 Facility System Safety. The system safety process consists of a series of analytical steps that are defined in the following paragraphs and shown in Figure 4-1.

- DEFINE THE SYSTEM by describing the physical and functional characteristics of the system employing the information available, and relate the interaction between people, procedures, equipment, and the environment.
- IDENTIFY HAZARDS related to all aspects of the operation (including both nominal and emergency operations) and determine their causes.
- ASSESS HAZARDS to determine their consequence severity and probability of occurrence, and to recommend means for their elimination or control.
- RESOLVE HAZARDS by implementing corrective measures to eliminate or control the hazards or assuming the risk.
- FOLLOW-UP analyses to determine the effectiveness of preventive measures and address new or unexpected hazards; issue additional recommendations if necessary.

4.2.2. Center System Safety Program Plan. A Center System Safety Program Plan (SSPP) specifies how the Center will meet its program system safety goals and objectives. The SSPP identifies key items such as the organizational structure, functional responsibilities and tasking, program milestones, deliverable data items, and analysis methodologies and techniques that will be employed during the life cycle of the facilities/modifications at the center.

The SSPP is the most important element in implementing a system safety program. The SSPP becomes the formal document that describes the planned safety tasks required to meet NASA safety requirements. The SSPP outlines organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other engineering and management activities. The SSPP does the following:

- Sets forth the safety program objectives;
- Defines the organizations which will perform the safety tasks;
- Defines the functional interfaces with other organizations (internal and external);
- Defines the tasks necessary to achieve the objectives and describes an integrated effort within the organization;
- Specifies the management review process and the system safety management controls during all center activities including new facility acquisition, existing facility modification, and all center operations;

DEFINE THE SYSTEM

Define the physical and functional characteristics and understand and evaluate the people, procedures, facilities, equipment, and environment



IDENTIFY HAZARDS

Identify hazards and undesired events
Determine the causes of hazards



ASSESS HAZARDS

Determine Severity
Determine Probability
Eliminate/control or accept the risk



RESOLVE HAZARDS

Implement corrective action
- Eliminate
- Control
or assume risk



FOLLOW-UP

Monitor for effectiveness
Monitor for unexpected hazards

System Safety Process
Figure 4-1

- Describes the technical methods for conducting safety analyses during the facility life cycle;
- Identifies any unusual safety activities that must be performed as a result of state of the art development or application; and
- Defines the data requirements and describes the necessary outputs.

The SSPP describes in detail how to manage and accomplish the detailed system safety tasks. For all NASA Center Directorates and contractors, the Center SSPP provides a means to understand how facility system safety is to be accomplished, and how system safety activities will later be audited. See Table 4-1 for a sample SSPP table of contents.

4.3 NASA SAFETY POLICY AND REQUIREMENTS

4.3.1. Roles and Responsibilities. NASA Policy Documents (NPDs) provide safety policy for the effective application of system safety throughout NASA. Emphasis is given to safety research, accident investigation, risk assessment, information exchange, safety motivation, training, and appraisal. Each Center implements the policy set forth in the NMIs by developing tailored management instructions that meet the desired goals and objectives of the Center.

NASA Centers direct policy and are held accountable for the specific functions of their System Safety program. The goals and objectives of each Center must include safety in orbital, facility, and research programs as well as other programs. NASA establishes system safety as an integral element of every program, starting in the requirements phase and continuing throughout the disposal phase.

4.3.2 Requirements Documents. NASA Headquarters requires that each Center follow the requirements of “NASA Safety Policy and Requirements Document,” NHB 1700.1 (V1-B); Occupational Safety and Health Administration; and requirements of other Federal, State, and local regulatory agencies. A documentation tree showing the hierarchy of NASA safety related requirements and guidelines is depicted in Figure 4-2.

The objective of the NASA Safety Program as outlined in the “NASA Safety Policy and Requirements Document” is "to positively effect the overall success rate for missions and operations and to prevent injury to personnel and loss of property and/or technical reputation." The NASA Headquarters Safety and Risk Management Division (Code QS) within the Office of Safety and Mission Assurance (SMA) has authority and responsibility for safety policy and oversight.

Table 4-1 -- Sample System Safety Program Plan Table of Contents

TABLE OF CONTENTS
NASA CENTER SYSTEM SAFETY PROGRAM PLAN

Preface

Scope

1. General
2. Purpose
3. Organization of Plan

References

Definitions

1. Government Documents
2. Commercial Publications

NASA Center Description

1. History
2. Organizational Structure
3. Operations
4. Maintenance
5. System modifications

NASA Center System Safety Activities

1. Management
2. Methodology
3. Safety Tasks
4. Task Matrix

Safety -Related Activities of Other Organizations

1. Safety-related tasks
2. Task Matrix

System Safety Program Plan Implementation and Maintenance

1. Program Schedule
2. SSPP Update
3. Safety Audits

System Safety Program Plan Application

1. New Systems
2. Existing Facilities and Systems
3. Operational Systems
4. Occupational Health & Safety
5. Construction Safety
6. Fire Protection
7. Safety Information and Reporting
8. Safety Training

Appendices

1. Acronyms/Abbreviations
2. Safety Checklists
3. Glossary

For the latest Safety and Mission Assurance
Documentation Tree click below

<http://www.hq.nasa.gov/office/codeq/qdoc.pdf>

Figure 4-2

The highest level of authority and responsibility for safety at the Center is the Center Director who delegates safety responsibilities at his installation. Delegated safety responsibilities include providing safety oversight for all activities, ensuring the safety of Center operations/programs, and implementing the provisions of “NASA Safety Policy and Requirements Document,” NHB 1700.1 (VI-B). Management Instructions are developed by each Center to define the Center safety policy, responsibilities, and the implementation process to incorporate the requirements.

NASA Headquarters policy requires that the Safety and Mission Assurance (SMA) Directors at each Center functionally report to the NASA Code Q/Office of Safety and Mission Assurance (SMA). The Office of SMA plans, directs, and evaluates NASA-wide SMA activities. The Office of SMA has established a requirement to incorporate safety, reliability, and quality into programs at their earliest stage and to develop standards and guidelines tailored to meet unique program requirements.

4.3.3 References. A list of the documents, guidelines, and good industry practices used to implement NASA facility system safety programs are provided below. This list is not comprehensive; however, it does include the most commonly used references at NASA Centers.

4.3.3.1. Required Documents

NASA Documents

- NHB 1700.1 (VI-B), “Safety Policy and Requirements Document”
- NSS 1740.11, “Safety Standards for Fire Protection”
- NHB 2710.1, “Safety and Health Handbook”
- NPG 8820.2, “Facility Project Implementation Handbook”
- Applicable Center Handbooks and Management Instructions

Other Agency Documents

- Title 29 Code of Federal Regulations (CFR) for Occupational Safety and Health
- Uniform Federal Accessibility Standard (UFAS) under the Americans with Disabilities Act (ADA)
- National Fire Protection Association (NFPA) Codes and Standards
- Standard Building Code adopted by the Center, such as:
 - Uniform Building Code (UBC)
 - Uniform Fire Code (UFC)
 - Uniform Mechanical Code (UMC)

4.3.3.2. Guidelines

- American National Standards Institute (ANSI) Standards
- American Society of Heating, Refrigeration and Air-Conditioning Engineers, Inc. (ASHRAE) Handbook and Standards

4.3.3.3. Industry Practices

- Department. of Labor/OSHA publications
- American Council of Governmental Industrial Hygienists (ACGIH) publications
- ACGIH Industrial Ventilation: A Manual of Recommended Practice
- NFPA Fire Protection Handbook
- National Safety Council (NSC) data sheets and publications
- NSC Fundamentals of Industrial Hygiene
- National Institute of Occupational Safety and Health (NIOSH) publications

CHAPTER 5

FACILITY SYSTEM SAFETY PROCESS

5.1 INTRODUCTION

System safety engineering, as presented earlier in this document, is an approach used to identify deficiencies in system or facility design/acquisition, facility modification, associated testing, and operational sequences, which can result in an element of risk. System safety is used to assess risk by examining all elements and their interaction in the operating environment. A system safety program ensures the integration of safety within the facility acquisition process. The objectives of a facility system safety program are:

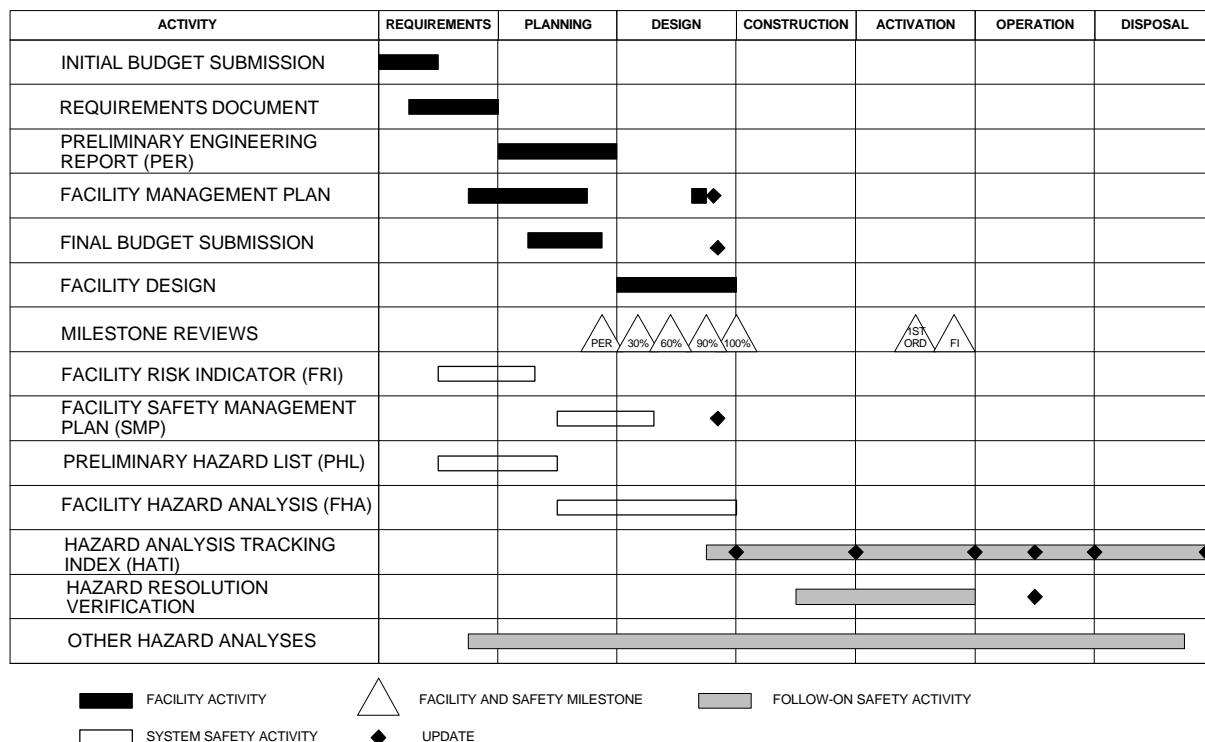
- To ensure that hazards inherent to the design, equipment, and intended use of the facility are eliminated, or the resultant risk is controlled to an acceptable level;
- To maximize operational readiness and mission protection through mishap prevention measures by ensuring that appropriate hazard control measures are designed and constructed into the facility in a timely manner and at minimum cost;
- To reduce safety and occupational health retrofit and modification requirements after the design stage;
- To ensure that safety and occupational health lessons-learned from previously constructed similar facilities are incorporated in facility designs; and
- To ensure that modifications do not increase the risk level of a facility.

All facility acquisition schedules and descriptions of facility acquisition activities are taken from NPG 8820.2, "Facility Project Implementation Handbook." NASA has seven facility project modification or construction phases: requirements, planning, design, construction, activation, operation, and disposal. Facility system safety activities take place concurrent with the normal facility acquisition process. These activities are shown in Figure 5-1.

The importance of the review process cannot be overemphasized; safety retrofit costs incurred in the operations phase can be two to ten times the cost of changes incurred during the design phase.

5.2 REQUIREMENTS PHASE


5.2.1. Initial Budget Submission. The Center Director provides the initial budget submission for the Construction of Facilities (CoF) project. This submission provides appropriate facility planning and budget documentation depending on the type of project. The required documentation is listed below.



Facility Acquisition Milestone Activities
Figure 5-1

- A long form write-up is required for discrete projects at or over \$1,500,000 and for land acquisition at any cost.
- A NASA Form 1509 (see Figure 5-2) should be completed to the extent possible for projects over \$200,000 not to exceed \$1,500,000 (budget year minor projects).
- A facility project cost estimate (NASA Form 1510 in NPG 8820.2).
- A project list (NASA Form 1514 in NPG 8820.2).
- A project-by-project list of the resources required for the preparation of Preliminary Engineering Reports (PERs) or final designs.

Even though safety costs are not a line item on the NASA Form 1509, the initial budget submission should also account for expected safety management expenses. Figure 5-3, "Initiator's Safety Checklist For Procurement," is an example form to start early hazard identification.

 National Aeronautics and Space Administration		Facility Project Brief Project Document				PROJECT CODE																																										
		DATE		SUB/REV. NUMBER																																												
PROJECT TITLE						INSTALLATION/PROGRAM OFFICE																																										
<div style="display: flex; justify-content: space-between;"> <div style="width: 40%;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;"></th> <th style="width: 50%;">ITEMS (LIST)</th> <th style="width: 40%;">AMOUNT</th> </tr> </thead> <tbody> <tr> <td rowspan="3" style="text-align: center; font-weight: bold;">APPROVED FACILITY PROJECT COST ESTIMATE</td> <td style="height: 30px;"></td> <td></td> </tr> <tr> <td style="height: 30px;"></td> <td></td> </tr> <tr> <td style="text-align: right;">TOTAL</td> <td></td> </tr> </tbody> </table> </div> <div style="width: 55%;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2" style="text-align: center;">RELATED COST DATA (Not included in the Approved Facility Project Cost Estimate, but required to make the facility initially operable)</td> </tr> <tr> <td colspan="2" style="text-align: center;">RELATED COSTS INVOLVED</td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input type="checkbox"/> YES (Identify) <input type="checkbox"/> NONE </td> </tr> <tr> <td style="width: 10%;"></td> <td style="width: 40%; text-align: center;">ITEM</td> <td style="width: 10%; text-align: center;">AMOUNT</td> <td style="width: 10%;"></td> <td style="width: 40%; text-align: center;">ITEM</td> <td style="width: 10%; text-align: center;">AMOUNT</td> </tr> <tr> <td rowspan="4" style="text-align: center; font-weight: bold;">TO BE PURCHASED TRANSFER OF EXCESS EXISTING</td> <td></td> <td></td> <td></td> <td style="text-align: center;">FUTURE FUNDING</td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">ACTIVATION</td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">OTHER REAL ESTATE</td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">OTHER (Specify)</td> <td></td> </tr> </table> </div> </div>							ITEMS (LIST)	AMOUNT	APPROVED FACILITY PROJECT COST ESTIMATE					TOTAL		RELATED COST DATA (Not included in the Approved Facility Project Cost Estimate, but required to make the facility initially operable)		RELATED COSTS INVOLVED		<input type="checkbox"/> YES (Identify) <input type="checkbox"/> NONE			ITEM	AMOUNT		ITEM	AMOUNT	TO BE PURCHASED TRANSFER OF EXCESS EXISTING				FUTURE FUNDING					ACTIVATION					OTHER REAL ESTATE					OTHER (Specify)	
							ITEMS (LIST)	AMOUNT																																								
						APPROVED FACILITY PROJECT COST ESTIMATE																																										
							TOTAL																																									
RELATED COST DATA (Not included in the Approved Facility Project Cost Estimate, but required to make the facility initially operable)																																																
RELATED COSTS INVOLVED																																																
<input type="checkbox"/> YES (Identify) <input type="checkbox"/> NONE																																																
	ITEM	AMOUNT		ITEM	AMOUNT																																											
TO BE PURCHASED TRANSFER OF EXCESS EXISTING				FUTURE FUNDING																																												
				ACTIVATION																																												
				OTHER REAL ESTATE																																												
				OTHER (Specify)																																												
CATEGORY		JUSTIFICATION		WORK																																												
FUND SOURCE		TYPE		IDENTIFICATION																																												
SCOPE/DESCRIPTION																																																
BASIS OF NEED																																																
PER FINAL CONSTRUCTION ACTIVATION START REQUIRED OPERATIONAL	SUBMITTED BY	SIGNATURE AND TITLE	DATE																																													
		SIGNATURE AND TITLE	DATE																																													
	CONCURRENCE BY	SIGNATURE AND TITLE	DATE																																													
		SIGNATURE AND TITLE	DATE																																													
	JX CONCURRENCE	SIGNATURE AND TITLE	DATE																																													
		SIGNATURE AND TITLE	DATE																																													
	APPROVED BY	SIGNATURE AND TITLE	DATE																																													
	PROJECT STIPULATIONS: (a) UNFORESEEN PROGRAMMATIC Project Analysis Sheet attached, dated _____																																															
	(b) Notification of bid per NHB 8820.2, Par. 6.04-05 (c) Send copy to NASA HQ CODE JX (d) _____																																															

NASA FORM 1509 SEP 96 PREVIOUS EDITIONS ARE OBSOLETE.

NASA Form 1509 - Facility Project Brief Project Document
Figure 5-2

January 1998

1. THIS PROCUREMENT INVOLVED HAZARDS WITH:		OTHER SAFETY HAZARDS (SEE DEFINITIONS)																																				
EXPLOSIVE MATERIALS CORROSIVE MATERIALS FLAMMABLE MATERIALS TOXIC MATERIALS RADIOACTIVE MATERIALS CONTROLLED DRUGS ASBESTOS LITHIUM BATTERIES	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><th>YES</th><th>NO</th></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </table>	YES	NO																	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><th>YES</th><th>NO</th></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </table>	YES	NO																
YES	NO																																					
YES	NO																																					
2. THE PERFORMANCE ON THIS CONTRACT WILL BE ON-SITE YES <input type="checkbox"/> NO <input type="checkbox"/>																																						
NOTE: IF YOU HAVE CHECKED ANY OF THE ABOVE BOXES WITH "YES" OR IDENTIFIED OTHER HAZARDS, THIS PROCUREMENT REQUEST MUST BE COORDINATED WITH THE HEALTH AND SAFETY BRANCH, CODE 250.2.																																						
3. I HAVE REVIEWED THE SCOPE OF THE WORK CONTEMPLATED WITH RESPECT TO POTENTIAL HEALTH AND SAFETY HAZARDS INHERENT IN THE ACCOMPLISHMENT OF THE WORK AND ALSO ANY SUBSEQUENT HANDLING, SHIPMENT, STORAGE AND UTILIZATION OF THE END PRODUCT. TO THE BEST OF MY KNOWLEDGE, THE ABOVE IS CORRECT.																																						
INITIATOR'S SIGNATURE	CODE	TEL. EXT. DATE																																				
(FOR HEALTH, SAFETY, AND SECURITY OFFICE ONLY)																																						
4. SAFETY REQUIREMENTS ARE RECOMMENDED AS FOLLOWS: <ul style="list-style-type: none"> <input type="checkbox"/> SAFETY AND HEALTH CLAUSE (NFS 1852.223.70) <input type="checkbox"/> SAFETY AND HEALTH PLAN REQUIRED (NFS 1852.223.73) <input type="checkbox"/> POTENTIALLY HAZARDOUS ITEMS CLAUSE (NFS 1823.370) <input type="checkbox"/> HAZARDOUS MATERIAL AND IDENTIFICATION AND MATERIAL SAFETY DATA CLAUSE (FAR 52-223-3) <input type="checkbox"/> SAFETY PRECAUTIONS FOR DANGEROUS MATERIALS (ARTICLE NO. H-110) <input type="checkbox"/> RADIOACTIVE MATERIALS (ARTICLE NO. N-113) <input type="checkbox"/> SAFETY AND HEALTH (ARTICLE NO. H-108 (A. <input type="checkbox"/> B. <input type="checkbox"/> C. <input type="checkbox"/>) STANDARDS ATTACHED YES <input type="checkbox"/> NO <input type="checkbox"/> <input type="checkbox"/> PROCUREMENT OF POTENTIALLY HAZARDOUS ITEMS (ARTICLE NO. H-111) <input type="checkbox"/> PROVIDING LITHIUM-SULFUR DIOXIDE AND LITHIUM-THIONYL CHLORIDE BATTERIES (ARTICLE NO. H-112) <input type="checkbox"/> DRUG CONTROL OFFICER APPROVAL (SEE GHB 5150.1, "SPECIAL APPROVALS") <input type="checkbox"/> IF THIS IS A COMPETITIVE PROCUREMENT, USE "SAFETY AND HEALTH PERFORMANCE HISTORY" AS AN "OTHER FACTORS" FOR EVALUATION <input type="checkbox"/> OTHER (SEE ATTACHED) 																																						
5. HEALTH AND SAFETY BRANCH (SIGNATURE)	DATE																																					
<p style="text-align: center;">DEFINITIONS</p> <p>Hazardous material is a substance or material in a quantity/form which may pose an unreasonable risk to health and safety or property. A list of materials that are hazardous may be found in 49CFR 172.101. Typical hazardous materials are those that may be highly reactive, poisonous, explosive, flammable, corrosive, reactive, produce contamination or pollution of the environment, or cause adverse health effects of unsafe conditions.</p> <p>Hazardous operations are those that involve the use of handling of hazardous materials or involve the use of other materials, phenomena, or elements at abnormal environmental or physical parameters that require special precautions. Some examples are high-pressure gas operations (in excess of 150 psig), low pressure high volume gas operations, voltage above 550 volts, storage or handling of propellants, chemicals or explosives, use of "heavy lift" material handling equipment, high or low temperature environments, environments with less than 19.5% or more than 25% oxygen by volume at normal pressure, forced variations of gravity, and excess radiation, vibration, or noise.</p>																																						
REVISED 10/96 THIS FORM MUST ALSO BE COMPLETED AND FORWARDED WITH THE PROCUREMENT REQUEST.																																						

Example Initiator's Safety Checklist for Procurement

Figure 5-3

5.2.2. Environmental Projects and Studies. Coordinate all environmental projects and studies with the NASA Safety and Environmental Offices at the Centers. The NASA Safety and Environmental Offices will provide guidance on the documents required for submitting environmental projects.

5.2.3. Requirements Document. The requirements document is essentially an update and expansion of a facility concept study (the initial preparatory work on a facility) with a major emphasis on the project description. The requirements document incorporates the results of any preliminary engineering reports or studies that have been completed and provides detailed criteria (e.g., size, location, environmental requirements, etc.) for each of the rooms, activities, or functions included in the facility. The requirements document will include elements such as:

- A narrative description of the purpose and/or function of the facility;
 - The physical dimensions of the area including ceiling or hook height;
 - The number and type of personnel assigned to the area;
 - Environmental requirements;
 - Process power, grounding, and lighting requirements;
 - Fire protection requirements;
 - Communication system requirements;
 - Special structural requirements;
 - Security requirements;
 - Material handling requirements;
 - A listing of major items of process equipment to be installed;
 - Environmental pollution control requirements; and
 - The identification of the present location of the activity.
- The requirements document is the primary input to the Preliminary Engineering Report.

5.2.4. Facility Management Plan. The facility project management plan establishes the schedule for implementation of a facility project and assigns responsibility and authority for various actions. The plan also provides a detailed outline of the steps in the facility implementation process, with provisions for well defined milestones to measure progress. It serves as the principal tool for determining work progress and establishes priorities for allocation of resources to ensure that the project is completed on time. During implementation of the facility project, the plan is updated, expanded, and used to maintain the overall project status during the budget process and the design, construction, and operation phases. NASA Headquarters must approve the project management plan for projects having a total cost of \$5,000,000 or greater. The plan includes:

- Identification of individuals or organizations responsible for project implementation;
- A description of the functional requirement including the operational need date, and, if required, the schedule for joint or beneficial occupancy dates (see NPG 8820.2);
- A description of the planned facility including capacity, scope, location, special features, and current cost estimates;
- An identification of all environmental requirements;
- The development of an acquisition plan ensuring that the funding method supports the operational need date(s); and
- Network or bar-type charts depicting a time-phased schedule with intermediate milestones.

The facility project management plan is not required for projects less than \$5,000,000, but is recommended and should contain adequate details based on project complexities.

5.2.5. Facility Risk Indicator (FRI)

5.2.5.1. Purpose of FRI. The FRI is a first step to estimating the combined level of risk associated with a facility. The FRI assessment classifies the severity of potential hazards inherent to the facility itself: its operations, processes, environment, equipment, potential interfaces, and personnel. Although the FRI can be performed at any time during the Facility Life Cycle, the FRI is generally performed early in the acquisition program during the conceptual phase to ensure potential hazards are identified. The FRI is the initial safety assessment used to help determine the level of system safety effort required to meet NASA safety requirements. This process begins by identifying hazards that may exist at any given point throughout the life of the facility. The FRI evaluation alerts the Facility Project Manager and other acquisition managers of the potential safety concerns within a facility.

The extent to which system safety analysis is applied to facility acquisition is initially based upon the FRI assessment. The FRI is categorized into four risk indicators ranging from a FRI of 1 (High Risk) to a FRI of 4 (Minimal Risk). A FRI of 1 signifies major risk associated with personnel safety, operational productivity, design effectiveness, environmental impact, and/or other user interfaces. A FRI of 4 indicates negligible or low risk. The potential hazards inherent to the facility are evaluated using the following criteria as evaluation factors:

- Life Safety - hazards which could potentially cause death or serious injury to personnel;
- Mission Continuity - failures which could have serious impact on mission capability and/or operability;

- Facilities Protection - failures which could cause serious damage to facilities or equipment resulting in significant financial loss; and
- Environmental Impact - hazards which could have serious impact to the adjacent facilities or operations or to the surrounding community.

The primary objective of the FRI for a facility acquisition project is to identify the potential risk involved with the facility and to ensure that the Facility Project Manager appropriates adequate funding to address safety concerns. By considering the size and complexity of the project and the safety risks associated with the project, this assessment will help identify the system safety activities, which should be accomplished early in the acquisition process and how resources should be allocated.

5.2.5.2. FRI Assessment Classification. The FRI process shown in Figure 5-4 has been developed to allow a project initiator to easily and quickly determine a facility FRI. The facility/project will be assigned a FRI from 1 (highest possible risk) to 4 (lowest possible risk), based on inherent hazards present in the facility, and their impact on facility protection, operational purpose of the facility, and personnel safety. Suggested guidelines for defining FRI categories and the applicable safety activities are listed below.

FRI 1 (HIGH RISK)

Definition. There is a high probability that hazards in this facility can cause loss of life. Hazards may result in loss of life, permanent disability, or serious occupational illnesses to one or more persons, three or more lost-time injuries, loss of facility operational capability for one month or greater, or damage to equipment or property in excess of \$500,000.

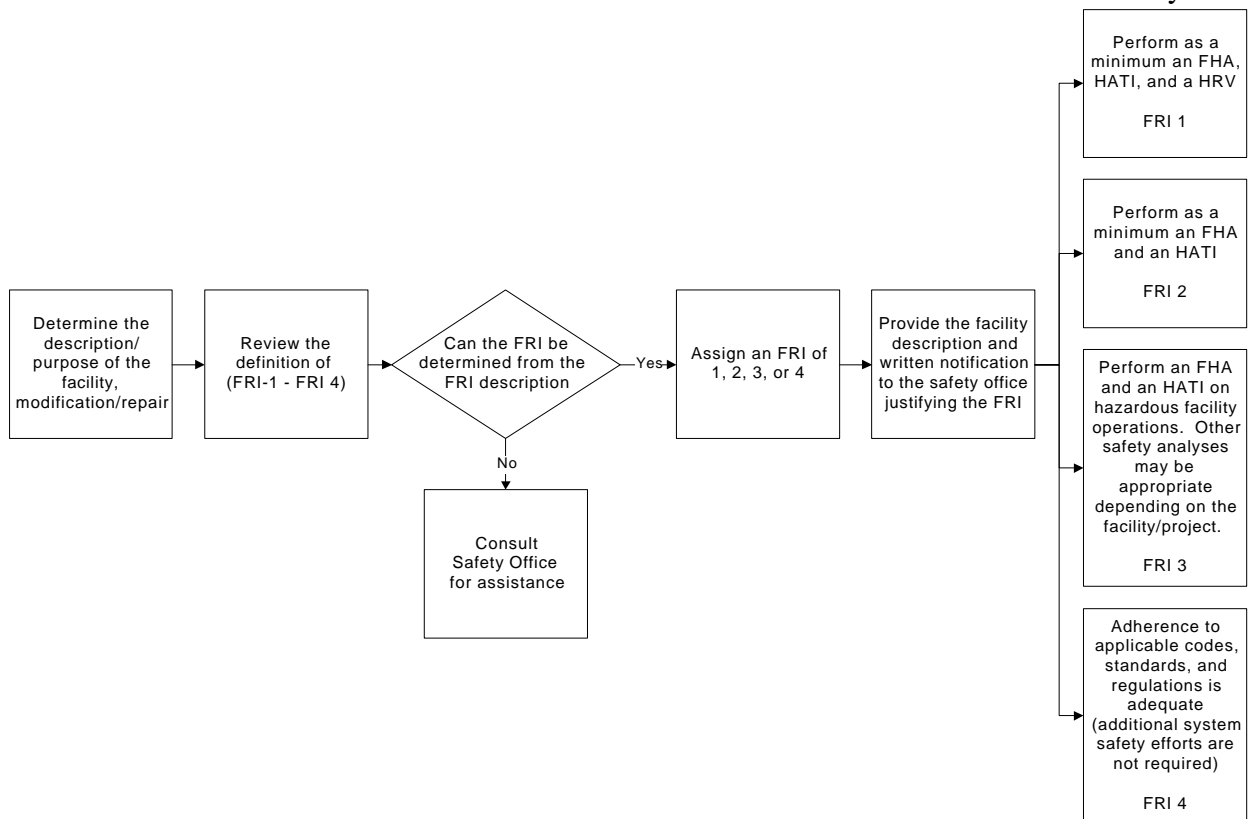
Safety Program Requirements. A Facility Safety Management Plan (FSMP) should be prepared. As a minimum, a Facility Hazard Analysis (FHA), Hazard Analysis Tracking Index (HATI), and Hazard Resolution Verification (HRV) should be done.

FRI 2 (MEDIUM RISK)

Definition. There is a medium probability that hazards in this facility can cause loss of life. Hazards may result in permanent disability to one or more persons, hospitalization (associated with illness or injury) of three or more persons, up to two lost time injuries, loss of facility operational capability from 2 to 4 weeks, or damage to equipment or property from \$250,000 to \$500,000.

Safety Program Requirements. A FSMP should be prepared. As a minimum, a FHA and HATI are recommended.

January 1998



Facility Risk Indicator (FRI) Process

Figure 5-4

FRI 3 (LOW RISK)

Definition. There is a low probability that hazards in this facility can cause loss of life. Hazards may result in hospitalization to one or two persons, occupational injury or illness resulting in a lost workday or restricted duty case, loss of facility operational capability from 1 day to 2 weeks, or damage to equipment or property from \$25,000 to \$250,000.

Safety Program Requirements. A FHA and HATI are recommended on hazardous facility operations. Other analysis methodologies may be appropriate depending on the facility or modification/repair.

FRI 4 (ACCEPTABLE RISK)

Definition. Loss of life as a result of hazards in this facility is unlikely. Hazards may result in no lost workday injuries or no restricted duty cases, loss of facility operational capability of less than 1 day, or damage to equipment or property less than \$25,000.

Safety Program Requirements. Adherence to applicable codes, standards, and regulations is adequate.

The FRI process (Figure 5-4) begins with a review of the proposed facility or project description. Often the FRI can be determined based on comparing the information presented in the facility description to the FRI categories presented in the previous paragraphs. However, some facility descriptions are not adequate to determine the FRI and additional research is required to determine the classification of the facility or project. A review of a checklist, such as the “Typical Energy Sources Checklist” provided in Appendix A, can assist in determining the FRI for the facility or project, particularly if the Center Safety Department helps with the evaluation.

A Facility Risk Indicator summarizes potential hazards inherent to a facility and its operation. This technique is used to rank hazardous aspects of a specific facility and enables a determination of appropriate safety activities required to minimize potential hazards associated with the facility and its operation.

5.2.6. Preliminary Hazard List. The purpose of the Preliminary Hazard List (PHL) is to identify and list hazards or areas of concern likely to be present in the facility including the environment in which the facility will be located. The PHL is the baseline document for the facility system safety effort. The following identification methods are typically used to identify the hazards associated with energy sources, hazardous operations, or procedures, and potential accidents that may result in injury to personnel or damage to the facility.

- Surveying the site;
- Interviewing site personnel;
- Drawing on expertise in the subject area;
- Reviewing lessons learned;
- Analyzing similar facilities;
- Analyzing available technical data;
- Reviewing energy sources;
- Reviewing requirements documents; and
- Reviewing the Project Management Plan.

Alone, any of these methods will identify some hazards, but a logical completion of all or a combination of these steps will result in the development of a more thorough PHL. Once the PHL is completed it is used to help determine what hazards exist in a facility. The PHL also provides input for the Facility Hazard Analysis (FHA). The PHL can be prepared in any logical format that allows the free flow of ideas. An example of a completed PHL is provided in Appendix B. This list was derived from reviewing energy sources, equipment, operations, procedures, personnel interviews, and an experts panel. Each of the above listed hazard identification methodologies is described in the following paragraphs.

5.2.6.1. Research of Similar Facilities. New facilities often are built to house some existing operations, usually at or near the proposed site. If the entire operation is new, then similar or related operations and systems usually can be identified at other NASA Centers.

Existing facilities, proposed operations, and the proposed site should be reviewed looking for indications of potential hazards that could exist in the proposed facility. This is the most important step, as it provides first-hand invaluable information to the actual facility and operations.

5.2.6.2. Interviews With User Personnel. Interviews with personnel actually involved with the day-to-day operations of the new system or facility can often provide information that does not appear in planning or technical documentation. Operations personnel are often eager to provide input into the overall design process for the new system or facility since they will eventually be using the facility. For instance, an interview may determine that inadequate lighting has been a problem for workers. Potential hazards resulting from poor lighting should then be documented in the PHL and subsequently addressed in the Facility Hazard Analysis.

5.2.6.3. Experts Panel Meeting. One of the most successful methods to identify hazards related to a project can be accomplished by conducting an "Experts Panel" meeting. This meeting brings together project engineers, representatives from cognizant safety organizations, and users who know the system or facility under design, and personnel with expertise in some aspect of the system or facility. During a brainstorming session, the experts analyze the system and, based on their area of expertise, identify potential hazards for the new system or facility.

To prepare for a typical Experts Panel meeting, a system description and initial draft of the PHL should be developed. The draft PHL will serve as the outline for discussion during the meeting. The experts are provided with the system description and draft PHL prior to the meeting to prepare. Choice of the "experts" attending the meeting vary greatly depending on the type of facility or system and the personnel available; the expertise many times comes from surprising areas. For example, a former design engineer for a chemical processing plant with experience in flammable liquid/gas transferring operations may provide considerable valuable input into a PHL being conducted on the design of a fueling facility for a spacecraft propulsion system. Another engineer with several years of experience as an OSHA inspector may provide insight during the Experts Panel meeting for the development of a PHL for a machine shop.

The Experts Panel meeting provides the opportunity for an organized review of all subsystems within the system or facility. As a result, the PHL develops into a refined and more comprehensive PHL. Although use of additional hazard identification methods discussed in this section ensure a more thorough hazard identification process, the PHL produced as a result of the Experts Panel Meeting typically provides a very realistic list of the most significant hazards to be included.

5.2.6.4. Lessons Learned. Mishap data from the Lessons Learned Information System (LLIS) can be used to evaluate facts associated with mishap events that could have impact or provide information on controlling or mitigating hazards in like facilities. The primary, contributing and potential cause; and recommend corrective actions to prevent recurrence of specific and similar mishaps may be available in the LLIS.

5.2.6.5. Similar Facilities. Analyzing similar facilities is another method for gathering hazard information. For instance, a hazard analysis for a spacecraft integration facility may provide valuable data as a starting point for an aircraft integration facility PHL encompassing similar operations. It is important to note that hazards identified from previously developed hazard analyses require careful review to ensure applicability.

5.2.6.6. Technical Data. Codes, standards, and regulations provide useful information in identifying facility hazards. Documents may include: NASA Policy Directives (NPDs), NASA Procedures and Guidelines (NPGs), NASA Technical Standards (NTSs), American National Standards Institute (ANSI) standards, NFPA standards, American Society for Testing and Materials (ASTM) standards, OSHA regulations; and Environmental Protection Agency (EPA) regulations. There may also be recommended practices and guidelines from professional organizations that deal with specific items used in the facility.

5.2.6.7. Review of Energy Sources. A useful systematic approach to conducting an engineering review of a system or facility may include checklist-based analysis, such as the Energy Trace Barrier Analysis (ETBA) (see Paragraph 7.2 for more information). This methodology proposes that hazards in a system or facility will be caused by an inadvertent release of energy stored in the system, facility, or environment. Thus, if all sources of energy can be identified, then theoretically all potential hazards can be identified. After developing an understanding of the system or facility under study, checklists are reviewed for applicable potential hazard sources. This and other checklist methodologies provide further confidence that a thorough PHL is being developed (see Appendix A for a “Typical Energy Sources Checklist”).

5.2.6.8. Summary. The Preliminary Hazard List is conducted early in the system safety analysis phase. Usually an ETBA is conducted on the system to develop the list. The PHL is an initial hazard identification effort. It is the basis for the follow-on, in-depth safety analysis. The information generated from the PHL helps evaluate the initial design requirements, provide data for concept and trade-off studies, and provide information on specific safety concerns. (see Appendix B for a “Preliminary Hazard List Example - General Laboratory Facility”)

5.3 PLANNING PHASE

5.3.1 Preliminary Engineering Report. The Preliminary Engineering Report (PER) is a link between the pre-planning phase and the final design phase of a facility. The PER establishes a project cost by providing an engineering cost basis. The PER includes preliminary engineering studies, the analysis of alternatives, essential design requirements and criteria, schematic single-line drawings, siting information, outline specifications, and cost estimates. A preliminary engineering report provides:

- A basic source of necessary data and cost estimates regarding the facility work required to support budgetary or other proposals;

- A functional need and serves as a mechanism for its subsequent consideration;
- A comprehensive justification for the proposed facility;
- Early and timely development of the facility project or work package(s) to meet functional needs including analysis of alternatives;
- Criteria for preparation of final architectural engineering design drawings and specifications for an individual facility project and defines the work for the construction phase(s); and
- The design and construction steps to be followed such as work packages, construction management, schedules, and interior milestones for the execution of the project.

5.3.2 Final Budget Submission. The field installations make final budget submissions that provide the following budget year facility project information:

- An updated long form write-up for Headquarters supported discrete projects, including updated material that responds to questions raised by the senior management review;
- An updated NASA Form 1509;
- An updated facility project cost estimate, NASA Form 1510;
- An updated priority list, NASA Form 1514, in the same format as the initial submission and signed by the Center Director or designated representative; and
- PERs for discrete projects if required.

5.3.3. Facility Safety Management Plan. The Facility Safety Management Plan (FSMP) should be written to meet the requirements of NHB 1700.1 (V1-B), Chapter 8. According to NHB 1700.1 (V1-B) Paragraph 807:

“Field Installations shall document and maintain a written Facility Safety Management Plan (FSMP) for each major facility acquisition. This plan shall be used to implement tailored safety requirements, including organizational responsibilities, resources, milestones, methods of accomplishment, depth of effort, and integration with other program engineering and management activities and related systems.”

The plan should clearly indicate how acquisition of the specific facility or facility modification meets the requirements of the overall System Safety Program Plan for the Center. The FSMP should be started after completion of the PHL and should be complete at the 30% Design Phase. The basic objective is to document recommended safety efforts for the remainder of the life cycle of the facility.

The FSMP should document the facility hazard resolution process and define when hazards have either been closed, accepted, or eliminated. For example, the plan can state that if hazards appear closed on 90% design drawings, then the hazards are closed. Another plan might state that hazards will not be closed until they are actually inspected in the field (this method is advantageous for facilities with a FRI of 1). The plan will also define and establish the management authority for closing or accepting hazards.

A Hazard Analysis Sub-Committee (HASC) may be established by the plan to review all hazards and make recommendations to management. The HASC usually consists of representatives from the safety office, the user's group, the architecture and engineering firm, and the facility project manager.

For a FRI 1 or 2 facility acquisition project, the FSMP may include requirements for additional hazard analyses such as a Sub-System Hazard Analysis, or an Operating and Support Hazard Analysis; requirements for a Hazard Analysis Tracking Index; and requirements for incorporation of special testing requirements to assure that the proposed facility can operate safely. A sample Table of Contents for a FSMP for a FRI 1 Facility is provided as Appendix C.

The FSMP should provide a method to ensure that:

- A safe design is being implemented in a timely, cost-effective manner;
- Hazards associated with the facility, identified during the FHA, are tracked (using a Hazard Analysis Tracking Index) to ensure they are evaluated and eliminated or controlled to an acceptable level throughout the life cycle;
- Minimum risk is involved in the design, materials, testing, and operation of the facility;
- Changes to the design, made during construction or installation/testing, do not impact safety;
- Training is provided for personnel involved in hazardous operations and processes;
- Codes, standards, and regulations are met;
- Safety milestones meet facility program requirements;
- Safety in operation and maintenance is demonstrated and proved; and
- Safety in disposal of the facility is established with clear procedures and methods for facility disposal.

In summary, the FSMP should ensure that a tailored program is developed for the particular facility acquisition.

5.3.4. Facility Hazard Analysis (FHA)

5.3.4.1. Purpose of a FHA. The FHA is a preliminary hazard analysis performed during the planning and decision phases of an acquisition program. For NASA facilities, the FHA is the initial, and often the only, risk evaluation of a facility or facility modification. The analysis includes a preliminary assessment of the facility's systems and subsystems, operations, processes, equipment, building structure, personnel, environment, and materials. The FHA is built upon previous studies or assessments performed, i.e., FRI and PHL; however, this analysis is more detailed. When complete, the FHA is used to establish a Hazard Analysis Tracking Index and to update the FSMP that will identify additional analyses required, if necessary, during subsequent phases. This documentation provides useful safety input for the decision making process used in trade studies, design criteria, and operational goals.

The FHA is prepared to identify, evaluate, and make recommendations for the elimination, control, or acceptance of hazards that could potentially cause:

- Loss of life and/or serious injury to personnel;
- Serious damage to facilities and/or equipment resulting in large dollar loss;
- Failures with serious adverse impact on mission capability, mission operability, or public opinion; or
- Detrimental harm to the environment and the surrounding community.

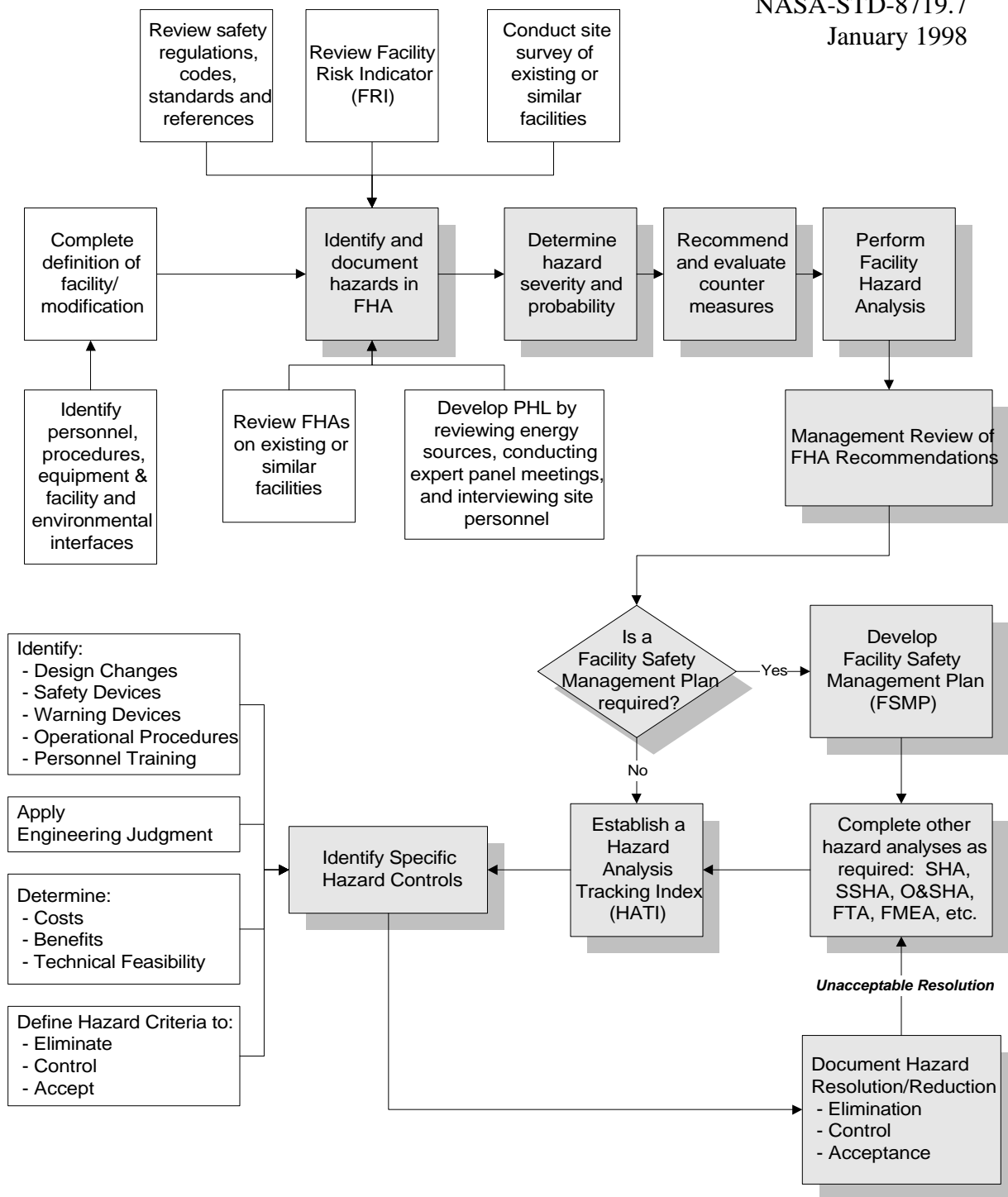
When the system safety effort is part of the overall design effort, the system safety engineers can participate in design review meetings and often consult with the designers throughout the FHA development. This arrangement provides the system safety engineer with a better understanding of all of the design considerations and how safety may play a part. Similarly, close contact with the system safety engineers provides the designers with a better idea of the major safety concerns being identified throughout the system safety analysis process. When the system safety effort is conducted independently from the design and the system safety engineer does not have access to the design engineers, then the analysis is usually less comprehensive and often results in unappreciated "surprises" for the facility designers.

5.3.4.2. Scope of an FHA. The FHA places the greatest emphasis on elimination/control of hazards early in the life cycle. The FHA is reviewed and revised several times to reflect the status of safety-related hazards that exist throughout the design cycle, i.e., during the 30%, 60%, 90%, and 100% design reviews; the completion of building construction; the end of system/subsystem installation; and prior to facility operations. Obviously, only a limited amount of information is available during the 30% design review. However, significantly more information is available during the 60% design review and should be reflected in the revised FHA.

Each revision consists of reviewing the identified hazards and modifying the status of those hazards that are either eliminated, controlled, accepted, or remain open for future consideration. It is essential to address each hazard as the design matures and to quickly report the status to management so that additional hazard analyses or design modifications can be performed before procurement and construction begin on the facility. This alleviates redesign efforts, maintains milestone objectives, and avoids unnecessary costs that could delay the completion and activation of the facility. The boundary of the FHA includes identification of hazards within the proposed facility, hazards external to the facility with respect to its physical location, and hazards related to the interface of the facility with the surrounding facilities and systems (i.e., fire protection water supply, electrical utility systems, transportation, and safe separation including explosives, hazardous materials, security, etc.). The FHA may also address environmental issues outside of the facility. Coordination between the Safety and the Environmental Offices at each NASA Installation establishes good practical judgment in examining environmental issues related to the facility.

5.3.4.3. Development of a FHA. The Facility Hazard Analysis process is shown in Figure 5-5. The initial step in the Facility Hazard Analysis uses various information to determine the hazards and level of risk associated with the facility and its operational use. The FHA is based on the best available data, including mishap and lessons-learned information. It is developed by:

- Reviewing design drawings, PER, requirements document, plans, etc..
- Reviewing applicable safety regulations, codes, and standards.
- Reviewing the Facility Risk Index and Preliminary Hazard List.
- Reviewing/conducting site surveys and interviews with proposed users.
- Reviewing historical data or lessons learned from existing or similar facilities.
- Identifying personnel, procedures, equipment, and facility interfaces.



Facility Hazard Analysis Process
Figure 5-5

Each hazard identified is documented in the FHA. The format should allow for the inclusion of the results of additional safety analyses (if needed), and the monitoring of the status of each hazard as the project proceeds from phase to phase.

5.3.4.4. Hazard Severity Categories. NHB 1700.1 (V1-B) defines four categories of hazard severity: Class I, Catastrophic; Class II, Critical; Class III, Marginal; and Class IV, Negligible. Figure 5-6 depicts these severity categories and provides a general description of the characteristics that define the worst-case potential injury or system damage if the identified hazard were to result in an accident.

5.3.4.5 Hazard Probability Categories. NHB 1700.1 (V1-B) includes guidelines showing

HAZARD SEVERITY

Class	Hazard Category	Definition
I	Catastrophic	May cause a permanent disabling or fatal injury to personnel, and/or loss of facilities, major systems, or associated hardware.
II	Critical	May cause severe injury or occupational illness, and/or major damage to facilities, systems, or hardware.
III	Marginal	May cause minor injury or occupational illness, and/or minor damage to facilities, systems, or equipment.
IV	Negligible	May cause first aid injuries or occupational illness, and/or minimal damage to facilities, systems, or equipment

Based upon: NHB 1700.1 (V1-B)

Hazard Severity Categories

Figure 5-6

how to determine a qualitative ranking of hazard probability. Failure rate data, if available, may be used to help make a decision regarding probability ranking; however, these data are most often not available for facilities. A probability ranking can be assigned for facility projects based on similar equipment and systems in similar facilities or historical safety data. Regardless of the method used, a probability ranking should be assigned because it is used in the risk definition to determine the potential hazards which must be addressed. Figure 5-7 shows the hazard probability classes typically used, and describes the characteristics of each level.

5.3.4.6. Hazard Risk Index. The Hazard Risk Index (HRI) is an application of the Risk Assessment Classification (RAC) system used to indicate the risk associated with each individual

HAZARD PROBABILITY

Estimate Level	Frequency of Occurrence	Definition	Fleet or Inventory
A	Frequent	Likely to occur immediately	Continuously experienced
B	Probable	Probably will occur in time	Will occur several times in the life of an item
C	Occasional	May occur in time	Likely to occur during the life cycle of the system
D	Remote	Unlikely to occur	Unlikely but possible in the life cycle of the system
E	Improbable	Is extremely unlikely	Extremely remote and is not expected to occur during the life cycle of the system

Based upon: NHB 1700.1 (V1-B)

Hazard Probability Categories

Figure 5-7





hazard. It is a number derived by considering both the severity and probability of a hazard, as shown in Figure 5-8. The HRI presents hazard analysis data in a format which helps the managing activity make decisions regarding whether hazards should be eliminated, controlled, or accepted.

As an example, a hazard such as a slip or fall due to wet or slippery floors could be assigned a severity level of III (Marginal), with a probability of A (Frequent). An explosion could be ranked I (Catastrophic), with a probability of E (Improbable). Looking at Figure 5-7 the slip or fall would have a HRI of 1 (Unacceptable), while the explosion would have a HRI of 3 (Acceptable with review by management).

This process provides the basis for logical management decision making, considering both the severity and probability of a hazard. It should be noted that, for valid risk assessment, the potential severity of a hazard may not be decreased unless physical changes are made to completely eliminate the hazards. However, the probability (and therefore the Hazard Risk Index) can be greatly reduced by design modification or by incorporating safety devices, warning devices, or special procedures.

HAZARD RISK INDEX MATRIX

Probability of Occurrence	Hazard Categories			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A - Frequent	1A	2A	3A	4A
B - Probable	1B	2B	3B	4B
C - Occasional	1C	2C	3C	4C
D - Remote	1D	2D	3D	4D
E - Improbable	1E	2E	3E	4E

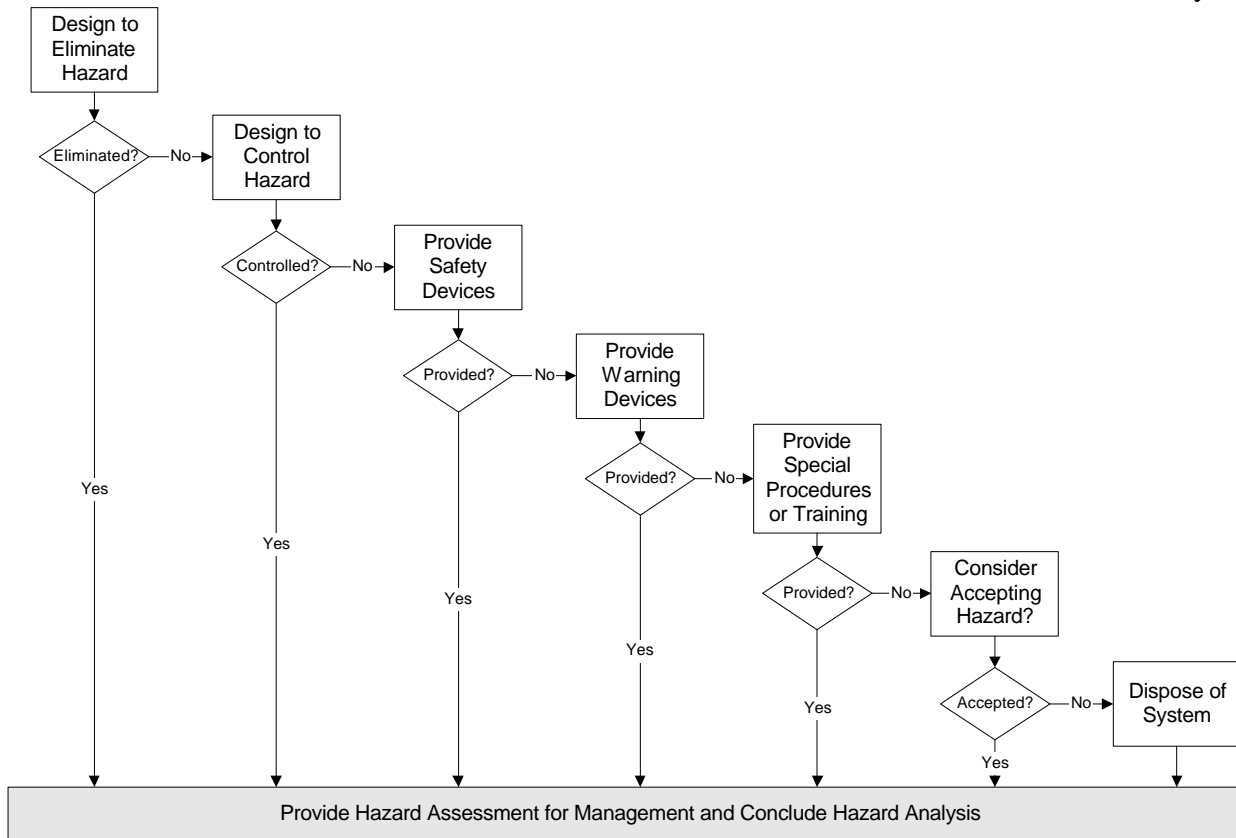
<u>Hazard Risk Index</u>		<u>Severity - Probability</u>	<u>Suggested Criteria</u>
1		1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
2		1D, 2C, 2D, 3B, 3C	Undesirable (Management Decision Required)
3		1E, 2E, 3D, 3E, 4A, 4B	Acceptable with Review by Management
4		4C, 4D, 4E	Acceptable without Review

Based Upon: NHB 1700.1 V1B)

Hazard Risk Index Matrix
Figure 5-8

5.3.4.7. Hazard Reduction Precedence. Risk management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. By assigning a HRI, a determination can be made as to whether hazards should be eliminated, controlled, or accepted. The process shown in Figure 5-9 helps to determine the extent and nature of preventive controls that can be applied to decrease the risk to an acceptable level within the constraints of time, cost, and system effectiveness. Hazard reduction strategies in descending order of precedence are listed below.

(a) Design to Eliminate Hazards. This strategy generally applies to acquisition of new equipment or expansion of existing facilities; however, it can also be applied to any change to equipment or facilities. The hazard source or the hazardous operation shall be eliminated by design without degrading the performance of the system or facility.



Hazard Reduction Precedence
Figure 5-9

(b) Design to Control Hazards. In cases where hazards are inherent and cannot be eliminated completely, they should be controlled through design. The major safety goal during the facility design process is to include safety features that are fail-safe or have capabilities to handle contingencies through redundancies of critical elements. Complex features that could increase the likelihood of hazard occurrence should be avoided. System safety analysis should identify hazard control, damage control, containment, and isolation procedures.

(c) Provide Safety Devices. Hazards that cannot be eliminated or controlled through design should be controlled through the use of appropriate safety features or devices. This could result in the hazard being reduced to an acceptable risk level. Safety devices (e.g., a pressure relief valve) are part of the system, subsystem, or equipment, and are an integral part of malfunction and emergency procedures during operations.

(d) Provide Warning Devices Where it is not possible to preclude the existence or occurrence of an identified hazard, visual or audible warning devices (e.g., a fire alarm bell) should be employed for the timely detection of conditions that precede the actual occurrence of the hazard. Warning signals and their application should be designed to minimize false alarms that could lead to secondary hazardous conditions.

(e) Provide Special Procedures or Training Where a hazard cannot be eliminated or controlled using one of the aforementioned methods, special malfunction or emergency procedures should be developed and formally implemented. These special operational procedures should be standardized and used in test, operational, and maintenance activities. For example, the user could be required to wear Personal Protective Equipment (PPE) (e.g., face shields, gauntlets, etc.).

(f) Hazard Acceptance or System Disposal Where hazards cannot be reduced by any means, a decision process must be established to document the rationale for either accepting the hazard or for disposing of the system.

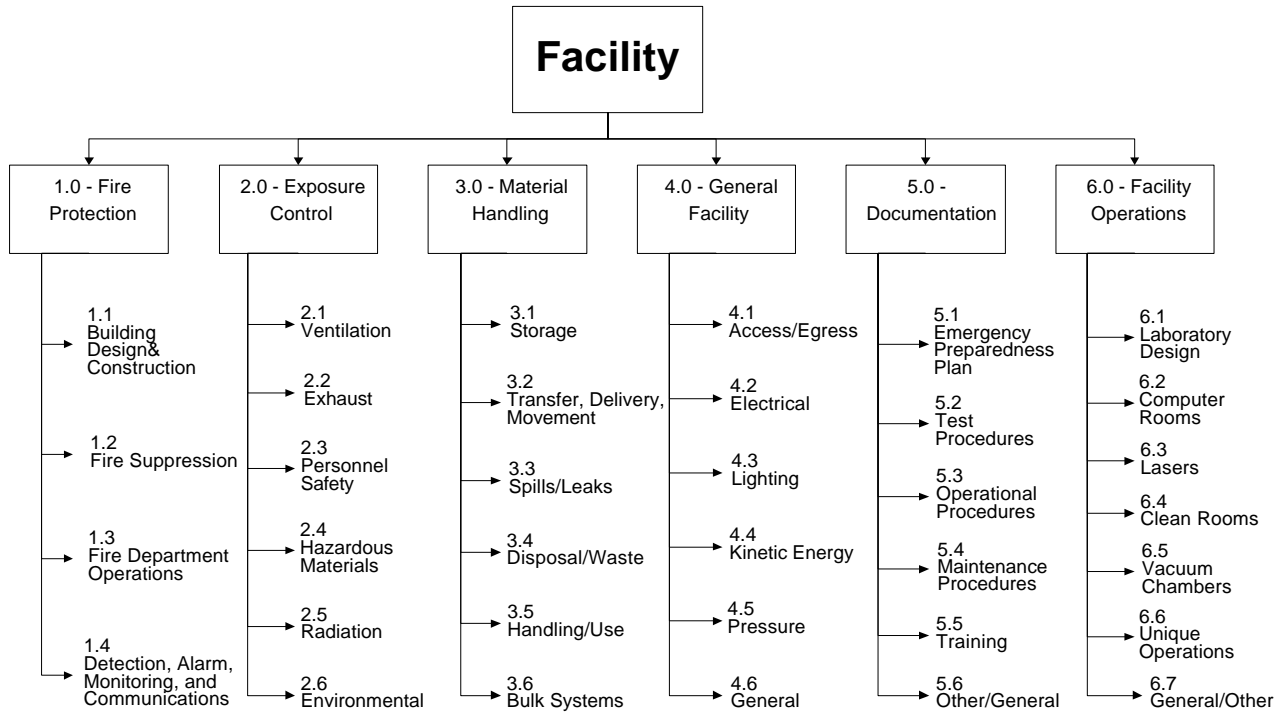
It should be noted that if the hazard cannot be designed out, a combination of hazard reduction controls including safety devices, warning devices, special procedures or training may be implemented.

5.3.4.8 Facility Hazard Analysis Data Sheets. The potential hazards identified in the FHA are organized by functional area. They are subdivided into different areas of concern, types of hazards, and/or design disciplines. This is illustrated in Figure 5-10, FHA Organization Tree. By organizing hazards into categories the Safety Engineer can cross reference the various hazard data entries shown in Figure 5-11, Facility Hazard Analysis Data Sheet. This ensures that each hazard category is identified and evaluated, preventing the possibility of over looking the hazard. The following is an explanation of the various entries in the data sheet:

(a) Heading. The heading on each FHA data sheet identifies the particular analysis. The "Project" for all data sheets should identify the name of the facility or project. The "Date" indicates the most recent version of each data sheet. The "System/Subsystem" will indicate the aspect of the facility covered by the FHA data sheet

(b) Control Number. The first column of the data sheet provides the "Control Number" for that particular hazard. The control number is related to the "System/Subsystem" provided in the heading, and to the corresponding number found in the FHA Data Sheet Organization on Figure 5-11.

(c) Hazard Description The second column, "Hazard Description," identifies the energy source that generates the hazard. This entry may also indicate the immediate cause for concern, such as a fire/explosion or toxic fumes buildup.



Facility Hazard Analysis Organization Tree
Figure 5-10

Project: _____			Facility Hazard Analysis				Revision : _____		Date: _____	
System/Subsystem: _____							Prepared by: _____		Page ____ of ____	
CONTROL NUMBER	HAZARD DESCRIPTION	CAUSES	EFFECTS	S-P 1	HRI 1	RECOMMENDATIONS	S-P 2	HRI 2	REFERENCES	STATUS

Facility Hazard Analysis Data Sheet
Figure 5-11

(d) Causes. The third column, "Causes," describes those items that create or significantly contribute to the existence of the hazard. This entry will usually include the major causes of the hazard, including items or conditions that increase the severity of the hazard.

(e) Effects. The fourth column, "Effects," describes the potential detrimental effects of the hazard, and analyzes the flow of energy between the source and the object that is to be protected. The data provided in this entry are used in assigning a severity to the hazard.

(f) S-P 1. The fifth column contains the Severity and Probability, "S-P 1," assigned to the hazard, based on Figures 5-6 and 5-7.

(g) HRI-1. The sixth column translates the "S-P 1" into a HRI of 1, 2, 3, or 4, as explained in Paragraph 5.3.4.6 and Figure 5-8. This first Hazard Risk Index (HRI-1) is assigned based on the assumption that no action has been taken to protect against the hazard. The HRI is used to assist management in deciding the best course of action for resolving the hazard.

(h) Recommendations. The seventh column, "Recommendations," provides recommendations, including design revisions or safety measures, to eliminate or control the hazard.

(i) S-P 2 and HRI-2. The eighth and ninth columns reflect the revised or residual Severity and Probability, "S-P 2," and Hazard Risk Index, "HRI-2," after the recommendation has been addressed and action has been taken to eliminate or control the hazard. It should be noted that for the S-P 2 the potential severity of the hazard cannot be decreased by design modifications or addition of safety measures; however, the probability of hazard occurrence can be greatly reduced, and thus, the Hazard Risk Index can be decreased.

(j) References. The tenth column, "References," cites the applicable required codes, standards, guidelines, and good industry practices upon which the recommendation was made (e.g., NFPA, OSHA 1910, UBC, UFC, etc.)

(k) Status. The eleventh column, "Status," lists whether the hazard is "OPEN," "CLOSED," or "ACCEPTED RISK" and to which phase of the acquisition process the hazard applies. The eleventh column includes an explanation of how and/or why the hazard is open or for a hazard to be closed, written documentation or verification is needed.

An example of a FHA is provided as Appendix D. (NOTE: Appendix D includes only representative hazards from the analysis, not the complete report).

5.3.4.9. Facility Hazard Analysis Scheduling. The FHA is a systematic safety analysis used to identify and document hazards, and to recommend countermeasures. The purpose of the

FHA is to identify hazards and all accompanying implications, to determine the severity and probability of the hazards, and to make recommendations for their elimination or control. The FHA should start in the planning phase so that safety considerations can be included in program planning, trade-off studies, and selection of design safety requirements. This will help reduce the possibility of costly design changes later in the development of the facility. The FHA provides a baseline of safety data from which further safety analyses can be conducted.

5.4 DESIGN PHASE

5.4.1. Facility Design. The facility design segment of facility acquisition is the stage in which the facility progresses from concept to actual design. For a much more detailed description, refer to Chapter 5 of NPG 8820.2, "Facility Project Implementation Handbook." Listed below are some of the activities performed and documentation prepared during the acquisition phase:

- Assignment of a Design Management Team;
- Determination of design parameters, standards, and considerations;
- Preparation of a design criteria package;
- Determination of design costs and funding sources;
- Procurement of Architect-Engineer (A&E) services;
- Value Engineering
- Field Installation Design Management
 - Design Reviews (30%, 60%, 90%, and 100%)
 - 100% Design (drawings and specifications); and
- Preparation of a Facility Acquisition Plan.

5.4.2. Hazard Analysis Tracking Index. A Hazard Analysis Tracking Index (HATI) (also referred to as a Hazard List Tracking Record (HLTR) in some NASA documentation) is a continuation of a Facility Hazard Analysis (FHA). The FHA data sheets provide the framework for the HATI. These data sheets are periodically updated to document actions taken to eliminate or control hazards. The HATI is part of the FHA, its purpose is to provide the user with a way to track the status of hazard resolution. Hazards identified by other hazard analysis techniques such as Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), or Operation and Support Hazard Analysis (O&SHA) are also added to the HATI for tracking.

5.5 CONSTRUCTION PHASE

This phase of the acquisition process is concerned not only with construction, but also the check-out of the facility with respect to the design drawings and specifications. Execution of the construction phase includes:

- Obtaining project approval (Facility Project-Brief Project Document NASA Form 1509) and funding (Resources Authority Warrant NASA Form 506A) or authority to advertise prior to receipt of funds;
- Management of the construction work;
- Completion of the facility;
- Preparation of operations and maintenance instructions and as-built drawings;
- Final inspection and acceptance of the facility construction work; and
- Final cost close-out.

Safety tasks during the construction phase focus on construction worksite safety, ensuring hazard controls are properly installed (through the HATI), and identifying hazards at interfaces and those resulting from change orders. Safety tasks include:

- Participate in the Pre-Construction Conference to insure the contractor's construction safety plan is appropriately developed;
- Construction shall not proceed until the contractor's safety plan is approved by the contracting officer in coordination with the Field Installation Safety Office;
- Ensure the application of all applicable building safety codes including the center's adopted codes as well as OSHA and NFPA regulations;
- Review equipment installation, operation, and maintenance plans to ensure all design and procedural safety requirements have been met;
- Evaluate mishaps or other losses to determine that adequate corrective action is implemented;
- Conduct construction or fabrication surveillance to include overseeing of construction worksite safety, safety program compliance reviews, and scheduled contract deliverables review and approval; and
- Update the HATI to identify any new hazards or closure of hazards that may result from change orders.

5.5.1 Hazard Resolution Verification. The purpose of the Hazard Resolution Verification (HRV) is to verify that all the "recommendations" of the FHA data sheets have been implemented and all hazards have been eliminated, accepted, or closed. The HRV is an important step in facilities ranked with a FRI of 1 because the potential number of hazards, and the severity and probability of hazards are greater. The HRV starts in the Construction Phase because this is the first phase in which hazards can be field verified for closure. The field inspection/verification is important to ensure that the safety controls have actually been put into place. The HRV also continues into the Activation Phase to ensure that the facility outfitting meets safety requirements. An example is the performance testing of a laboratory fume hood to ensure proper hood capture.

If the procedures in a building involve potential hazards, the HRV can be used to verify that steps outlined in a Safety Manual or Chemical Hygiene Plan are actually performed in day-to-day operations.

5.6 ACTIVATION PHASE

The final activity in the facility project process is the check-out and activation of the facility that was constructed as a result of the design drawings and specification. Some of these activities are:

- Development of the Facility Activation Plan;
- Facility safety review (Operational Readiness Review);
- Preparation of operation and maintenance instructions and as-built drawings;
- Subsystems and integrated systems tests;
- Final inspection and acceptance of the facility construction or installation work;
- Final cost close-out; and
- Facility outfitting. This includes laboratory installation of fume hoods, chemical Storage cabinets, equipment hookups, workbenches, etc.

5.6.1. Initial System Test / Operational Readiness Review. Facilities constructed for NASA Centers should be scheduled for inspection and acceptance after construction has been completed as described in the contract documents. This should occur before the facility is activated or used to accommodate the intended function. System safety is an integral part of the acceptance phase. Two important system safety steps in facility activation are: initial system test and operational readiness review.

Complex facilities with multiple interfaces, potential unidentified residual hazards, high energy sources, and a variety of controls and interlocks may require an Initial System Test (IST) prior to the Operational Readiness Review (ORR) to verify that all hazards have been identified and either removed or controlled, that the subsystems operate correctly, and that subsystem interfaces have been properly designed and constructed. Prior to commencing the IST, a hazard analysis shall be conducted to identify hazards created during testing and the controls devised to eliminate those hazards or reduce them to an acceptable level. FRI 1 facilities usually are candidates for an IST.

An ORR committee should be convened for facilities where there is a significant degree of risk of accident or improper operation that might cause personnel injury or death or serious damage to equipment, buildings, or adjoining areas. ORRs should also be convened if an IST has been performed.

The purpose of the ORR is to review the facility hazards documented in the HATI and controls, review the IST results if applicable, verify an initially safe operation, and make recommendations

to the Center Director for final decision and approval concerning status of residual hazards and any restrictions or limitations on the operation of the facility. The ORR committee should be composed of the appropriate facility managers, users, and safety personnel. For less hazardous operations, the ORR is an informal review by a team composed of construction inspectors, safety personnel, and others as appropriate. This team reviews the hazards and controls, verifies an initially set operation, and makes recommendations to the Facility Project Manager for final decision and approval concerning status of residual hazards and any restrictions or limitation on the operation of the facility.

5.7 OPERATIONS PHASE

The Operations Phase is the normal operations and use of the facility. The normal facility operations begin once the facility has been formally approved, and finishes at the time of facility disposal. Repair, maintenance, and rehabilitation are normal events during the life of a facility.

During the Operations Phase, the system safety work does not end. The HATI should be updated as facility changes are made. Any modifications made to the original design, or new activities performed in the facility, should be reviewed by the safety staff to assure that any new hazards or mitigated safety controls are accurately reflected in the HATI. Annual facility walkthroughs also help the safety engineer keep abreast of any changes in the facility. As required, a formal Operating and Support Hazard Analysis may need to be performed of the activities in the facility.

5.8 DISPOSAL PHASE

The Disposal Phase of the facility is the actual decommissioning of the buildings and facilities. In the disposal phase of the life cycle the potential safety and environmental aspects should be evaluated. Some of the concerns may be: residual ionizing radiation sources, heavy metals, toxic chemicals, and asbestos. When required, a formal hazard or environmental analysis may be needed. The results of the analysis and courses of action to abate a hazardous situation should be an integral part of the facility disposal plan. Safety and environmental personnel should monitor hazardous conditions to ensure compliance with applicable laws and regulations.

Safety related concerns during the disposal phase include the procedures to be used for dismantling the facility, the equipment required such as cranes and heavy equipment, security during the disposal process, training for the team responsible for dismantling the facility, disposition of the equipment in the facility, disposal of hazardous materials, logistics, and making the facility safe and ready for the next tenant (assuming that the facility will not be destroyed). The Facility System Safety Program Plan for the facility will have to be modified to identify the analysis methodologies appropriate for the decommissioning of the facility. All identified hazards should be resolved.

CHAPTER 6

OTHER FACILITY ACTIVITIES REQUIRING A SYSTEM SAFETY INPUT

6.1 INTRODUCTION

Facility system safety programs that result in the highest practical level of safety within the constraints of time, cost, and system effectiveness are dependent on emphasis given to other facility acquisition plans, procedures, and activities. Operating procedures, maintenance procedures, facility acceptance plans, training plans, configuration management plans, emergency management plans, and facility decommissioning plans must be included in the facility acquisition program for the facility to function successfully throughout its life cycle. System safety inputs to each of these disciplines are described in the following paragraphs.

6.2 OPERATING PROCEDURES

Operating procedures for facility equipment such as air handling equipment, fume hoods, fire/emergency management systems, and fire detection and suppression systems are usually provided by the manufacturer. These procedures, which generally have to be made facility-specific, must be reviewed to assure that appropriate hazard warnings and cautions provided by the manufacturer are included. Additionally, procedures must be reviewed to ensure that hazards identified in either the Facility Hazard Analysis or other facility specific hazards analyses that are related to procedures are addressed. Typical hazards identified in Facility Hazard Analyses include requirements for PPE; requirements for special tools, certification, or licensing; requirements for operating certain equipment; and requirements for emergency instructions including egress.

6.3 TEST ACTIVITIES

NASA is currently pursuing various advanced missions. To develop the appropriate technology for these missions, NASA conducts intensive ground testing. NASA performs both manned (frequently using astronauts as test subjects) and unmanned testing. Manned tests, many times, are conducted in oxygen-enriched and/or pressurized environments or neutral buoyancy tanks. Unmanned tests may use high pressure liquid hydrogen or oxygen, anhydrous ammonia, hydrazine, or other dangerous media. High temperatures, pressures, accelerations, and electrical potentials are typical in most NASA test operations. This requires a special test safety program. Because the NASA test environment can be hazardous and complex state-of-the-art hardware systems are used, the safety organization should develop an integrated, independent test safety program.

Test safety engineers operate at the "nuts and bolts" level and fully understand all systems and subsystems that will be tested. They also work with members of various divisions to help reach

the common goal of achieving a successful test. The safety organization should be completely autonomous of any test organization and reports to the Center Director. This maintains the necessary independence that is required for appropriate oversight. Reconciling these seemingly mutually exclusive relationships is key to providing a meaningful safety function.

Safety tasks are diverse over the hardware life cycle of pre-test, test, and post-test activities. Pre-test activities require the use of system safety techniques. Failure modes and effects analyses (FMEAs) and hazard analyses are the primary system safety methods applied for timely identification and control of hazards. Safety engineers support test activities through periodic real-time monitoring of various phases of test conduct. Review of post-test reports close the circle, furnishing safety information for improved future analyses. (Bahr, 1988)

6.4 MAINTENANCE PROCEDURES

Facility and equipment maintenance procedures must be developed for facilities and their operational systems to minimize risk to personnel and the facility. Maintenance activities play an important role among those normally expected events that occur during the life of a facility and so they too require procedures for hazardous tasks. Operational certification and calibration procedures for equipment such as cranes, fork lift trucks, functional test equipment, electrical cable repair, machinery repair, emergency systems maintenance, and other facility systems often require incorporation of appropriate warnings, hazards, and cautions. This can be accomplished by using a system safety approach to identify and control the operational hazards that occur before and during the use of such equipment. A system safety approach is essential since not all equipment is dedicated to a particular facility activity nor used by the same operator, and because it can be used for multiple facility operations.

A formal Operating & Support Hazard Analysis (O&SHA) should be performed to identify operational hazards with a high risk as required by NHB 1700.1 (V1-B), "NASA Safety Policy and Requirements Document." Equipment maintenance procedures should be provided for equipment that include controls identified in the O&SHA. These operating and maintenance procedures are often referred to as Hazardous Operating Procedures. They identify special cautions and warnings to personnel involved in performing the procedure; authorize standardized, acceptable work practices for maintenance; and verify systems/equipment, instructions for checkout, servicing, handling, and transportation. The information that is typically found in a Hazardous Operating Procedure is summarized below:

- Identification of specific hazards to which personnel will be exposed during the operation;
- Identification of the operating location for the hazardous task;
- Identification of hazard controls and a means for verifying that they are in place;

- Identification of safety precautions where specific guidelines must be observed or actions must be taken to prevent or limit the hazard;
- Identification of organizational elements and facilities required to support the operation;
- Identification of tools, equipment, and personal protective clothing;
- A list of referenced documents that contain instructions that support the operation;
- Unique safety rules and regulations that must be followed throughout the operation;
- A list of essential personnel required to support the operation;
- Identification of control areas to minimize risk to others;
- Identification of personnel required to be certified or licensed to perform the operation; and
- Identify emergency instructions.

6.5 FACILITY ACCEPTANCE PLANS

Facility acceptance is generally the responsibility of the Facility Project Manager, the assigned inspector, the contractor, and safety personnel. The objective of this inspection from the safety perspective is to verify resolution of identified hazards, to identify safety related defects and deficiencies, to schedule the necessary corrective action, and to update the Hazard Analysis Tracking Index (HATI). When conducting the inspection, safety personnel should verify that the specified safety features are provided in accordance with recommendations presented in the Facility Hazard Analysis, facility drawings, and specifications. The inspection should also include identification of safety deficiencies that could delay the installation of critical facility or mission equipment. It should also include the identification of instances where safety deficiencies would impose undue additional expense. The facility manager normally develops a schedule for work to be corrected and provides a schedule of the deficiencies to be corrected. When the facility manager and safety personnel are satisfied that the deficiencies have been corrected, the final inspection is scheduled. The final inspection date is generally established by the Facility Project Manager. The final inspection generally includes a tour of the entire facility project; verification of the corrected deficiencies previously identified in the HATI and FHA; and inspection of hardware, equipment, and operations (including installed equipment) for safety compliance. Safety related controls should be checked to assure they are in proper working order. If not, the final inspection report should include provisions for identifying those systems where the safety inspection will be made at a future date. Safety deficiencies not previously identified should also be included in the final report and entered in the HATI.

6.6 TRAINING PLANS

A well planned training program establishes requirements and minimum certification levels for personnel involved in potentially hazardous operations. Training procedures should place necessary emphasis on the safety aspects for all facility operations to help eliminate one of the most frequent causes of accidents - lack of knowledge or skill. If employees are expected to do their work safely, procedures must be developed to identify how the work is accomplished and to ensure that they have the knowledge and skill to perform the job in exactly that manner. Therefore, it is the responsibility of safety professionals and facility management to develop training procedures that encompass the safety needs of each person in the work place.

6.6.1. Operational Training. OSHA 1910.26, Section 21(b)(2), states "the employer shall instruct each employee in the recognition and avoidance of unsafe conditions and the regulations applicable to his/her work environment to control or eliminate any hazards or other exposure to illness or injury." Training procedures are required to ensure personnel are educated in the recognition and avoidance of hazards and should be developed throughout the life cycle of the facility. Early in the planning and design phases many hazards are identified, through analysis, in the FHA. These hazards may occur during facility construction, activation, maintenance, or disposal operations. The control measures identified through analysis are then developed to eliminate or prevent the occurrence or likelihood of accidents/failures. Not only do controls include design, operational, or personnel requirements, but they also include training of personnel to ensure they understand the facility systems and operations that they are going to operate. For example, a facility manager should ensure that training procedures are developed for every operation within his/her facility. This may include handling and storage of hazardous materials, operation of a laser laboratory, pressurizing flight test articles, operating motorized equipment, and operating electrically energized equipment.

6.6.2 Emergency Training. Training procedures are required for emergency situations that may occur within the facility. Such events are unexpected and personnel involved in the emergency response operations need to be able to respond immediately. They must also have the knowledge and skill required to react competently. Training procedures provide facility personnel who can respond to the emergency with the required information to perform as the situation dictates.

Emergency training procedures should be organized so the various steps or actions performed do not themselves create a hazardous situations. Also, these training events must maintain a logical framework for demonstrating sound safety practices. The FHA and the O&SHA are two types of analyses that may be used to identify what types of emergency procedures are necessary for the facility and also identify the logical framework for creating emergency procedures. System safety analyses ensure that all aspects of facility emergencies are recognized and assist in maintaining a safe and healthy work environment.

6.7 CONFIGURATION MANAGEMENT PLANS

The key provision of the Facility System Safety Program Plan should stipulate that an initial system safety analysis should be conducted for each facility, that a baseline for controlled documents be established, and that these analyses and documents be kept current by an active Configuration Management (CM) program. These analyses and the continuous update provided by the CM program provide procedural and risk information to operating personnel while recording and maintaining the current status of supporting documentation, equipment, and services within those facilities. CM implies control and continuous updating of documents and includes continuous systems safety analysis to assess the impact of change. It is important that any change to facility hardware, software, or procedures be processed through the CM program. Basic to any CM program is the notification of the change to the affected parties, verification that no protective measures have been degraded or defeated, and that no new hazards have been introduced.

Modifications to facilities are generally initiated by one of four methods. The method selected depends on the complexity and magnitude of the anticipated change. These four methods are:

- Administrative Change - Facility modifications that are administrative and do not affect safety. An example of this type of change is the replacement of a mechanical or electrical component with a like device (valve, meter, etc.)
- Center Facility Engineer Review Change - Facility changes resulting from a problem or failure that does not affect the facility baseline documents. These should be reported and reviewed by safety personnel
- Minor Change not Requiring Design Review - Facility modifications affecting the facility baseline documents and not requiring the Design Review Process
- Change Controlled by Design Review Process - Facility change requiring major modification during the Design Review Process

Risk review is another aspect of the CM program and all configuration changes submitted are subject to a system safety engineering analysis. During this process, standard operating procedures, checklists, and engineering drawings are analyzed to assess the impact of the change.

6.8 EMERGENCY MANAGEMENT PLANS

Emergency Management Plans are required in accordance with NPD 8710.1, "NASA Emergency Preparedness Program Policy."

Work on Emergency Management Plans for new facilities generally starts as early in the acquisition process as practical. The facility design should consider aspects of the proposed

facility that can have impact on the level of emergency response capability required, the parameters of possible emergencies, the coordination required with other organizations, and emergency response procedures.

Efforts to ensure adequate preparation for emergency situations should begin during the planning phase for new facilities, modifications to existing facilities, or facility/system rehabilitation. Preliminary Hazard Lists, Facility Hazard Analyses, and other hazard analysis techniques can identify hazards that can impact emergency response. Frequently recurring hazards include access/egress problems, ventilation and smoke control problems, communication system deficiencies, and fire detection/suppression system deficiencies. Guidelines presented to, and guidance presented by, the emergency preparedness planners are intended to help ensure the facilities and equipment needed to cope effectively with emergency situations are available and adequate.

Typical hazards that have applicability to emergency preparedness include:

- Fire protection equipment is selected/designed considering the emergency response requirements for the facility.
- Fire and smoke detection devices are located considering the layout and design of the facilities and the location of fixed hazardous equipment.
- Manual alarm devices that are of a type to discourage inadvertent activation.
- Facility layouts that do not allow accidental flammable liquid or vapor intrusion into an area where there is a potential for a serious fire or explosion. Specifications to minimize emergency conditions which could result from such hazardous liquid or vapor intrusion must be considered.
- Adequate water pressure is available for fire hydrants and standpipes. Additionally, hydrant locations related to the facility should be reviewed to assure that long hose runs are not required to reach the most hazardous areas of the facility.
- Roadways to the facility assure adequate access for emergency vehicles.

During the conduct of all Facility Hazard Analyses, the intended use of the facility should be reviewed with the emergency response organization on the NASA Center, and with local emergency response organizations who may provide assistance or back-up in the event of an emergency.