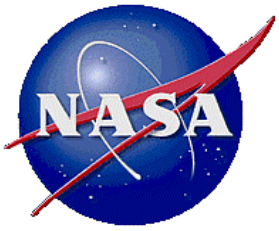


NOT MEASUREMENT SENSITIVE

National Aeronautics and Space Administration

NASA-STD-8719.7
January 1998

FACILITY SYSTEM SAFETY GUIDEBOOK

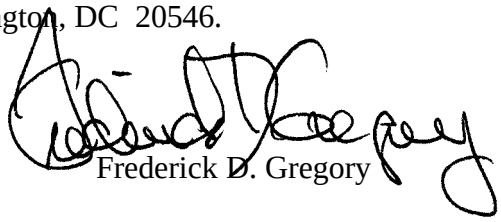
NASA TECHNICAL STANDARD

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

TABLE OF CONTENTS
(Continued)

PARAGRAPH **PAGE**

APPENDICES

APPENDIX **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

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;

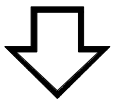
DEFINE THE SYSTEM

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

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 (V1-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:

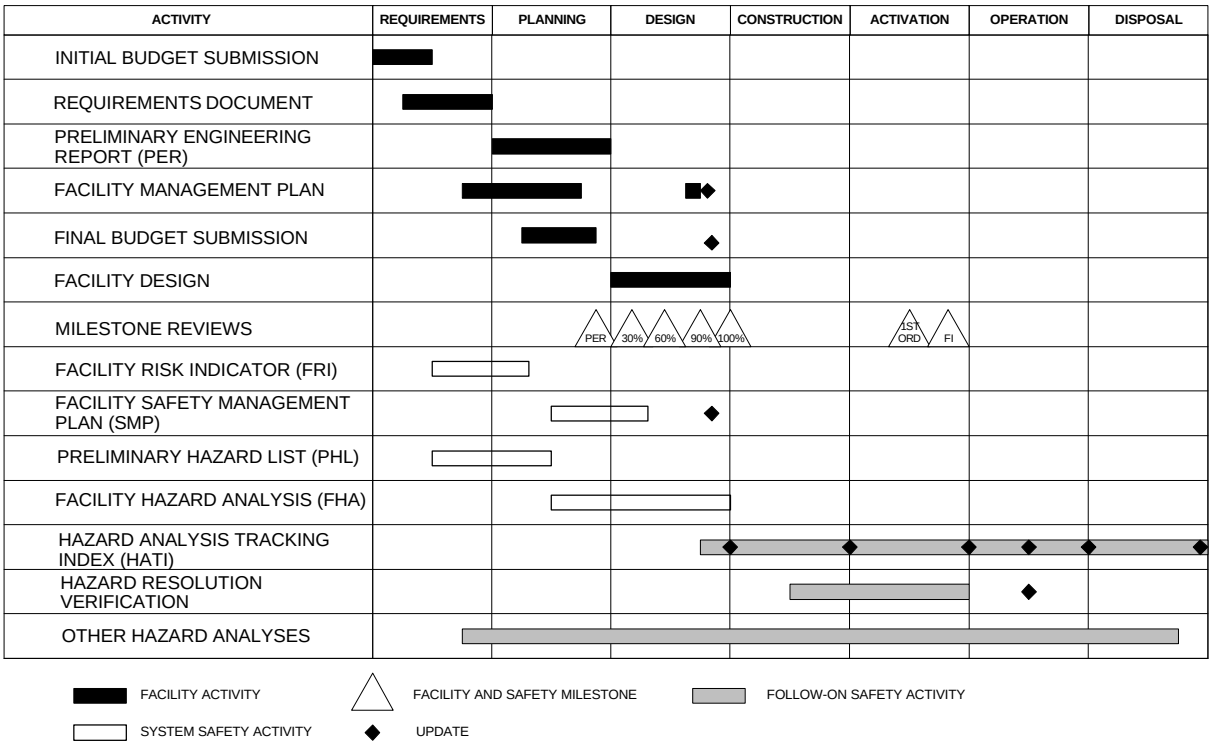
- To ensure that hazards inherent to the design, equipment, and intended use of the facility are eliminated, or the resultant risk is controlled to an acceptable level;
- To maximize operational readiness and mission protection through mishap prevention measures by ensuring that appropriate hazard control 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

RELATED COST DATA (Not included in the Approved Facility Project Cost Estimate, but required to make the facility initially operable)

RELATED COSTS INVOLVED ☐ YES (Identify) ☐ NONE | PER (Amount) | DESIGN (Amount)

APPROVED FACILITY PROJECT COST ESTIMATE	ITEMS (LIST)	AMOUNT
	TOTAL	
CATEGORY	JUSTIFICATION	WORK
FUND SOURCE	TYPE	IDENTIFICATION

ITEM	AMOUNT	ITEM	AMOUNT
TO BE PURCHASED		FUTURE FUNDING	
		ACTIVATION	
TRANSFER OF EXCESS		OTHER REAL ESTATE	
EXISTING		OTHER (Specify)	

SCOPE/DESCRIPTION

BASIS OF NEED

PER	START		
	COMPL		
FINAL	START		
	COMPL		
CONSTRUCTION	AWARD		
	COMPL		
ACTIVATION START			
REQUIRED OPERATIONAL			

SUBMITTED BY	SIGNATURE AND TITLE	DATE
CONCURRENCE BY	SIGNATURE AND TITLE	DATE
JX CONCURRENCE	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

1. THIS PROCUREMENT INVOLVED HAZARDS WITH:

	YES	NO		YES	NO	OTHER SAFETY HAZARDS (SEE DEFINITIONS)
EXPLOSIVE MATERIALS			OXIDIZING MATERIALS			
CORROSIVE MATERIALS			IONIZING RADIATION			
FLAMMABLE MATERIALS			NON-IONIZING RADIATION			
TOXIC MATERIALS			ELECTRO MAGNETIC RAD.			
RADIOACTIVE MATERIALS			SEVERE NOISE OR VIBRATION			
CONTROLLED DRUGS			CONFINED SPACES			
ASBESTOS			HI VOLTAGE (ABOVE 500V)			
LITHIUM BATTERIES						

2. THE PERFORMANCE ON THIS CONTRACT WILL BE ON-SITE YES □ NO□

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:

- □ SAFETY AND HEALTH CLAUSE (NFS 1852.223.70)
- □ SAFETY AND HEALTH PLAN REQUIRED (NFS 1852.223.73)
- □ POTENTIALLY HAZARDOUS ITEMS CLAUSE (NFS 1823.370)
- □ HAZARDOUS MATERIAL AND IDENTIFICATION AND MATERIAL SAFETY DATA CLAUSE (FAR 52-223-3)
- □ SAFETY PRECAUTIONS FOR DANGEROUS MATERIALS (ARTICLE NO. H-110)
- □ RADIOACTIVE MATERIALS (ARTICLE NO. N-113)
- □ SAFETY AND HEALTH (ARTICLE NO. H-108 (A. □ B. □ C. □) STANDARDS ATTACHED YES □ NO □
- □ PROCUREMENT OF POTENTIALLY HAZARDOUS ITEMS (ARTICLE NO. H-111)
- □ PROVIDING LITHIUM-SULFUR DIOXIDE AND LITHIUM-THIONYL CHLORIDE BATTERIES (ARTICLE NO. H-112)
- □ DRUG CONTROL OFFICER APPROVAL (SEE GHB 5150.1, "SPECIAL APPROVALS"
- □ IF THIS IS A COMPETITIVE PROCUREMENT, USE "SAFETY AND HEALTH PERFORMANCE HISTORY" AS AN "OTHER FACTORS" FOR EVALUATION
- □ OTHER (SEE ATTACHED)

5. HEALTH AND SAFETY BRANCH (SIGNATURE)	DATE

DEFINITIONS

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.

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 that 19.5% or more than 25% oxygen by volume at normal pressure, forced variations of gravity, and excess radiation, vibration, or noise.

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)

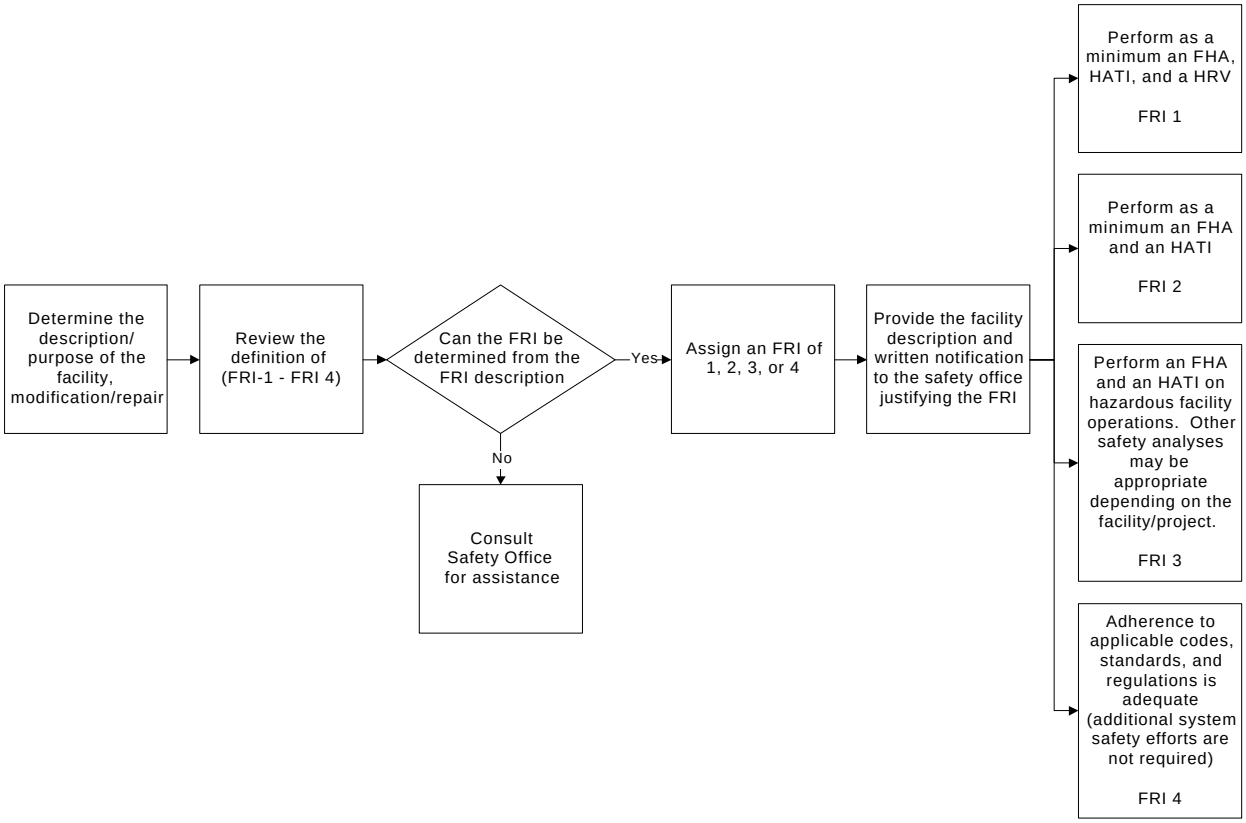
Definition. There is a high probability that hazards in this facility can cause loss of life. Hazards may result in loss of life, permanent disability, or serious occupational illnesses to one or more persons, three or more lost-time injuries, loss of facility operational capability for one month or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



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 Guidellines (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, sitting 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 pro 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.

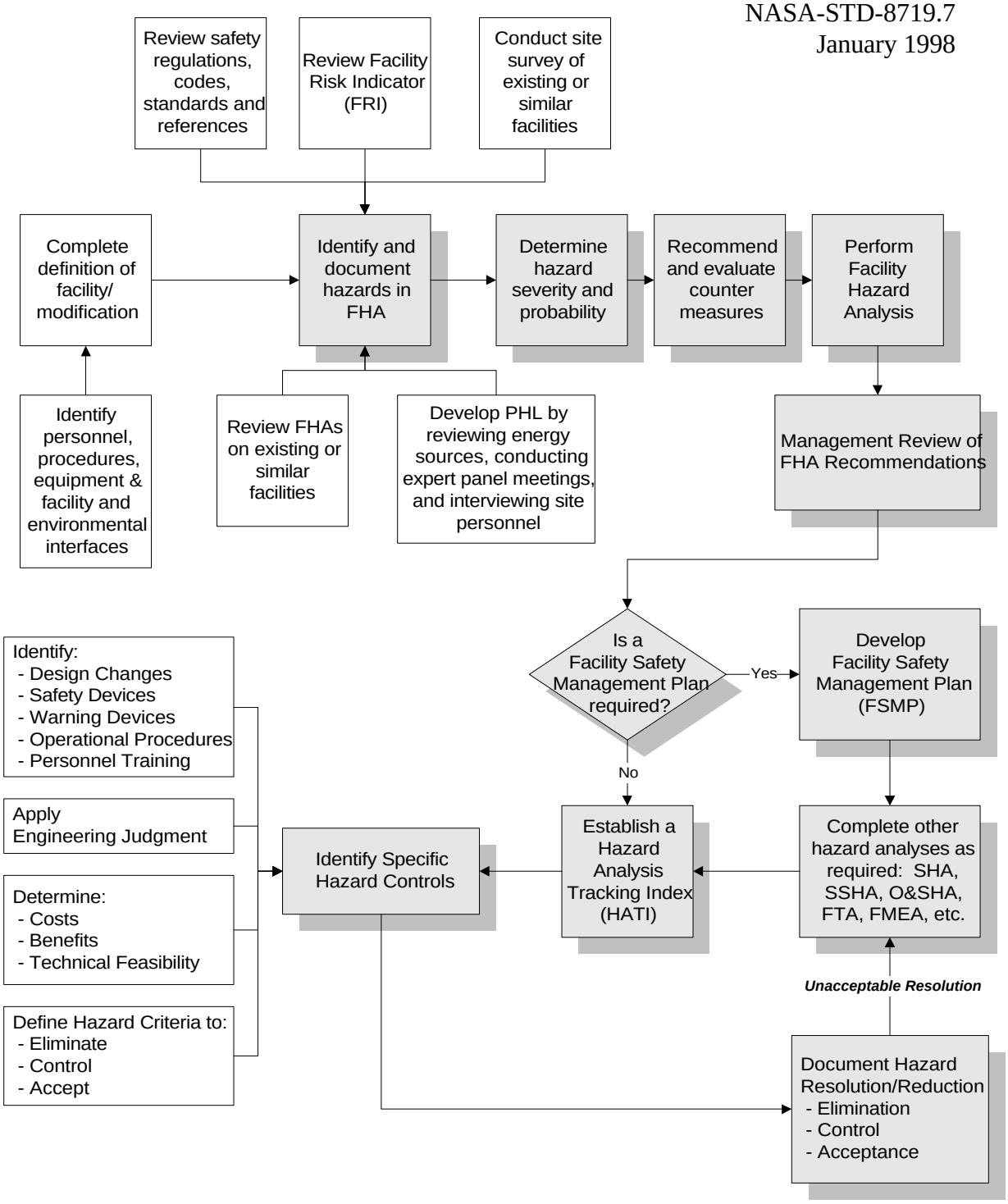
When the system safety effort is part of the overall design effort, the system safety engineers can participate in design review meetings and often consult with the designers throughout the FHA development. This arrangement provides the system safety engineer with a better understanding of all of the 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

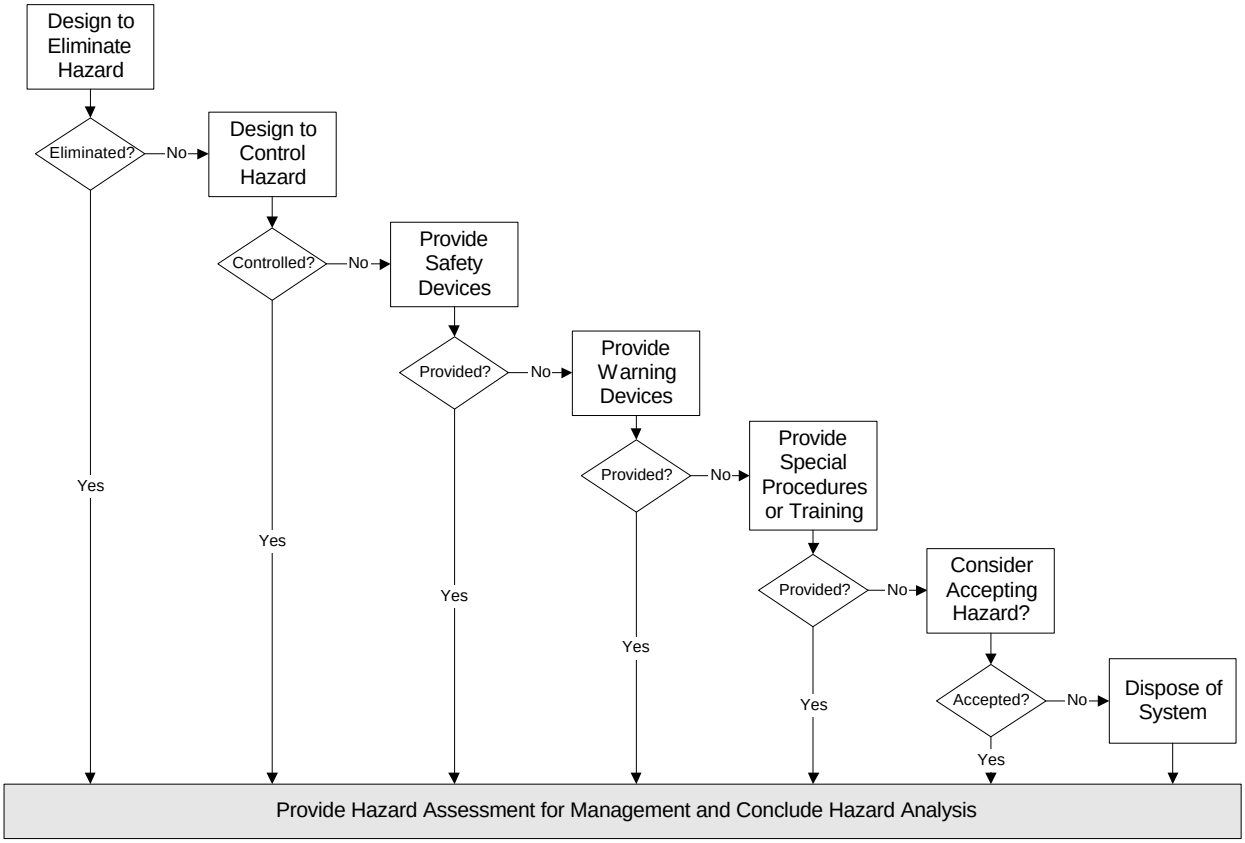
Hazard Risk Index		Severity - Probability	Suggested Criteria
1		1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
2		1D, 2C, 2D, 3B, 3C	Undesirable (Management Decision Required)
3		1E, 2E, 3D, 3E, 4A, 4B	Acceptable with Review by Management
4		4C, 4D, 4E	Acceptable without Review

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.

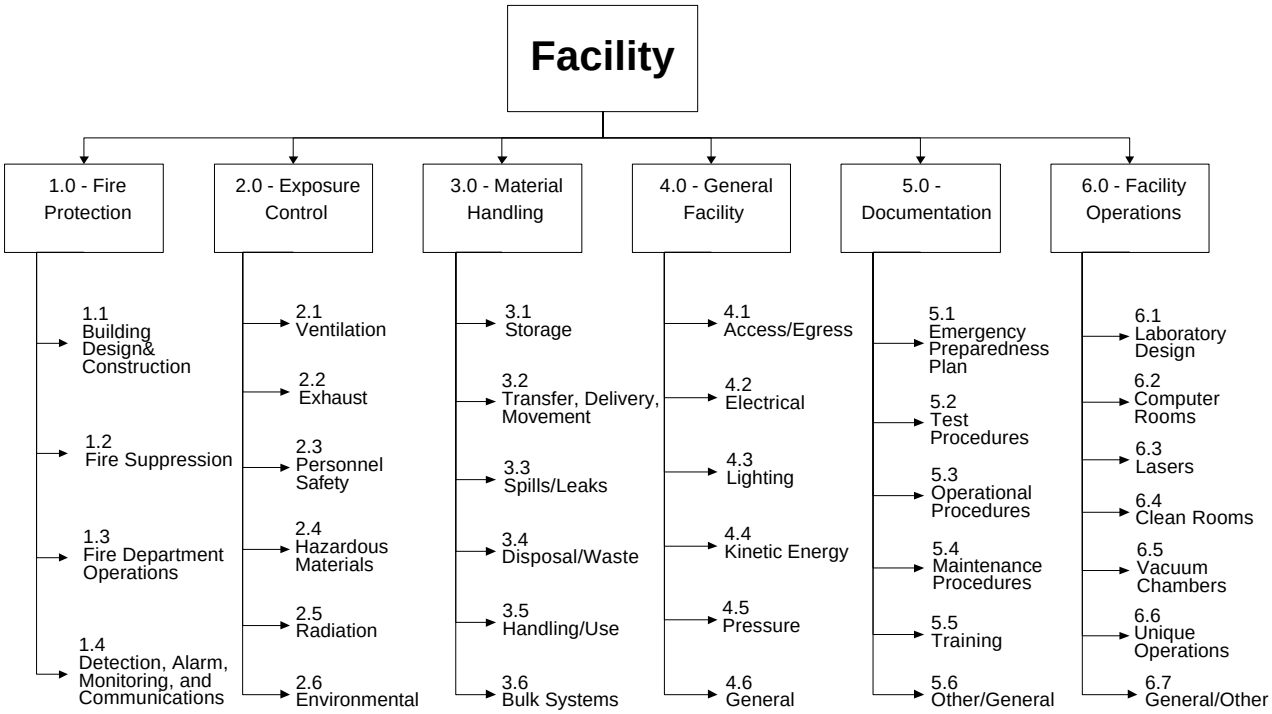
It should be noted that if the hazard cannot be designed out, a combination of hazard reduction controls including safety devices, warning devices, special procedures or training may be implemented.

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.

CHAPTER 7
OTHER HAZARD ANALYSIS METHODOLOGIES

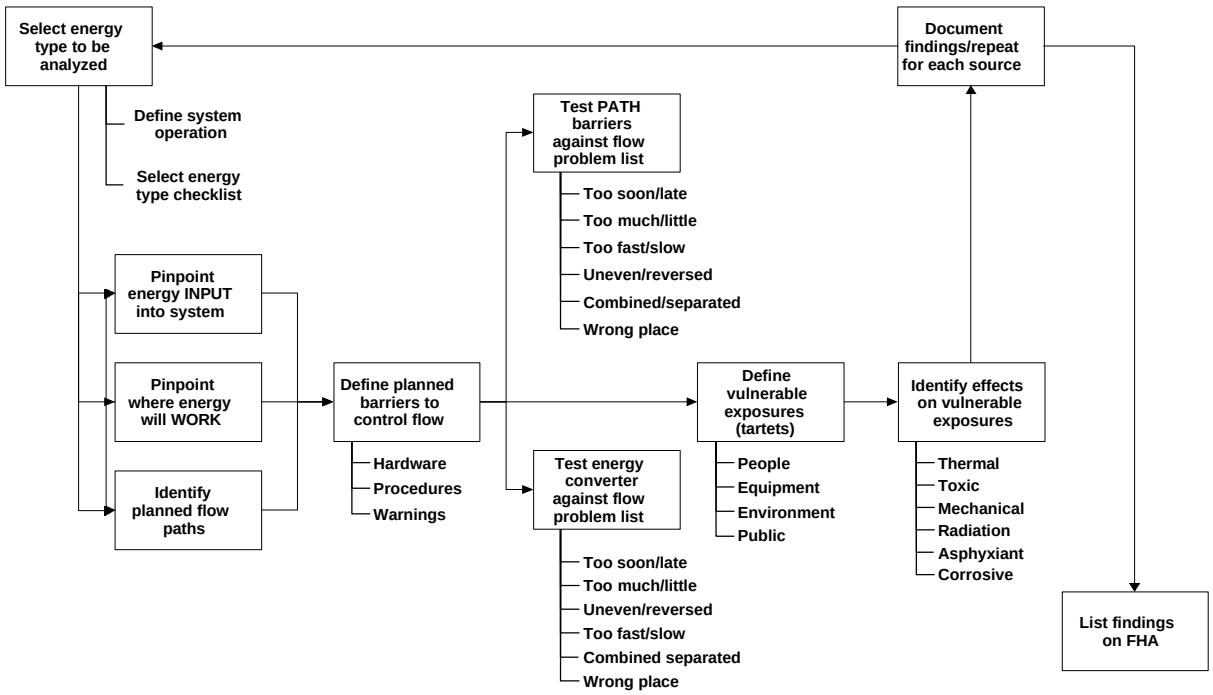
7.1 INTRODUCTION

Once initial system safety efforts are in progress, it may become necessary to do more in-depth analysis for the purpose of accurately assessing risk and controlling hazards. Eight of the more common in-depth risk analysis methodologies are described in the following paragraphs; any or all may be useful, depending on the facility and system life cycle phase, application, and operating environments.

7.2 ENERGY TRACE BARRIER ANALYSIS

7.2.1. Description. An Energy Trace Barrier Analysis (ETBA) is a qualitative analysis methodology used to develop more detailed knowledge of hazards. This technique shown in Figure 7-1 approaches the discovery of hazards by tracing the flows of energy into, through, and back out of a facility, system or operation. It is based upon the premises that:

- Mishaps arise from the risks within an operation.
- Mishaps interrupt or degrade the operation.
- Mishaps are an unwanted transfer of energy.
- The unwanted transfer of energy that produces injury to persons or property is due to a lack of barriers or controls over the energy.



Energy Trace Barrier Analysis Procedure
Figure 7-1

The ETBA process is particularly desirable and useful since it can be applied at any stage of the project to facilitate detailed analysis of those hazards discovered late in the project as well as those found at the beginning. The objective of ETBA is to find unsuspected hazards through methodical tracing of energy flows in the planned operation and across subsystem interfaces to locate potentially harmful diversions.

Each type of energy source, summarized in Table 7-1, should be considered individually from the perspective of the operations components and whatever subsystem energy control strategy may exist. The operation needs to be analyzed at the input/use/output level for each energy type to determine if the operation's plan or design addresses realistic potential control problems and satisfactorily controls them.

ETBA is used when concern over possible unacceptable loss indicates a need for better understanding of the operation. This is particularly true when lethal or significantly destructive energy flows characterize the operation and experience with the change or operation does not exist, or there has been a high loss rate, or behavior of certain energy interfaces is not known. ETBA is feasible because it is easy to identify the energy sources in almost any circumstance; the drawback is that performing an ETBA requires detailed familiarity with the operation or system. ETBA requires the services of someone who intimately understands the operation and can trace energies and barriers/controls thoroughly.

The ETBA is performed by tracing the sequence and logic of energy flow through the operation. For each energy type, the flow must be tracked to each transfer or use point, and each physical or procedural barrier to the energy must be considered to determine what harmful outcomes are likely to occur when:

- Too much or too little energy flows;
- The energy flows too soon, too late, or not at all;
- The energy flow is blocked or impeded in its pathway;
- The energy flow conflicts with another energy flow at a transfer or use point; and
- A barrier degrades, is disturbed, or does not function at all.

For a mishap to occur there must be an energy source with a release flow of energy to a target in the absence of adequate barriers. The flow or transfer of energy is the path between the energy source and the target or component of the operation being protected.

Table 7-1
Energy Types and Examples for Energy Traces
Caused by Internal Events:

1. Electrical
   - ac/dc flows
   - stored electric energy
   - electromagnetic radiation
   - static charges/flows

2. Mass/Gravity/Height
   - falls and drops
   - falling objects
   - falling hazardous materials

3. Rotational Kinetic
   - machinery
   - fans

4. Pressure/Volume & Kinetic Displacement
   - container ruptures and explosions
   - vacuum creation
   - liquids spill/flood
   - vapor expansion

5. Linear Kinetic
   - projectiles
   - rams, moving parts
   - shear press
   - vehicular movements, prints, pre-stressed members

6. Chemical Reactions
   - corrosion, oxidation, combustion, or
   - interactions among deposited materials,
   - polymerization,
   - decomposition,
   - toxic asphyxiant, anesthetic

Table 7-1 (cont.)
Energy Types and Examples for Energy Traces

7. Thermal
   heat, cold
   alternate heat/cold
   radiation/conduction/
   convection, sublimation

8. Etiologic
   viral,
   bacterial,
   fungal

9. Ionizing radiation
   gamma,
   alpha,
   beta

10. Noise and Vibration

11. Human Interactions

Caused By External Environmental Events:

1. Terrestrial
   earthquake, flood, landslide
   subsidence, compaction, cave-ins, water table

Caused By External Events

1. Radiation, explosions, projectiles,
   noise, vibration, fire

2. Atmospheric
   wind, rain, snow, lightning,
   hail, and acid rain

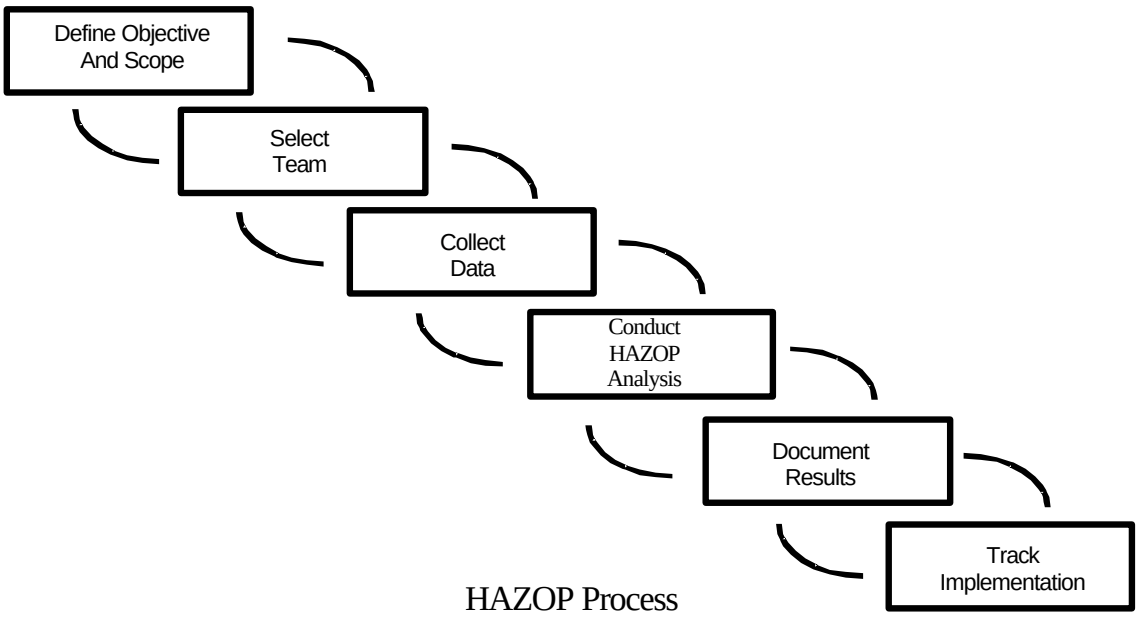
7.2.2. Results. In performing ETBA, an engineer develops and maintains a listing of energy sources and the hazards associated with each energy form source. Identified hazards are included in the Facility Hazard Analysis (FHA), or the Hazard Analysis Tracking Index (HATI) if the FHA is complete.

7.3 HAZARD AND OPERABILITY STUDY

7.3.1. Description. The Hazard and Operability (HAZOP) Study is a qualitative method of analysis used in identifying risk related to highly hazardous substances. The method provides a means of identifying a multitude of process hazards. It is used to identify potential hazards and operability problems early in the acquisition cycle at the time of design development of a process. Since the method can be applied early, the potential cost needed to eliminate or correct the hazard is minimized. The HAZOP is performed by an interdisciplinary team of experts who systematically examine each part of a process. This team identifies how deviations from the design intent can occur and whether the collective or individual deviations can create hazards.

The HAZOP is a structured group analysis technique for stimulating one's imagination in order to identify and assess the significance of all the ways a process unit can malfunction or be improperly operated. Its purpose is to identify potential process hazards due to system interactions or exceptional operating conditions.

The analysis objectives are to identify deviations from the design intent of the system. Then the analyst determines the safety concerns associated with the identified deviations. Finally, recommendations are proposed for resolving safety concerns or accepting risk. The HAZOP process is shown in Figure 7-2 below.



HAZOP Process
Figure 7-2

An optimum team should range in size from four to eight members and include designers, operators, and users.

The first step in a HAZOP is to identify the "node" to be analyzed. Some of the key items used in selecting nodes are:

- The next design change placed on the system,
- When a significant change of state occurs,
- Separate equipment items, and
- Different processes

Once a node has been selected, it is analyzed with respect to guide words with the process conditions. Guide words (no, more, less, reverse, etc.) are coupled with process conditions (flow, pressure, temperature, etc.). Table 7-2 offers a simplified application.

Table 7-2 - Guide/Process Condition

GUIDE WORD	PROCESS CONDITION
No	Flow
More (High, Long)	Pressure
Less (Low, Short)	Temperature
As Well As	Level
Part of	Time
Reverse	Composition
Other Than	pH

Guide Word plus Process Condition = Deviation

When organizing a HAZOP team one should consider the members' experience and background. Once a guide word is combined with each process condition the team brainstorms the possible deviations leading to bad consequences. One example is high pressure leads to:

- Death, personnel injury.
- Property damage.
- Environmental damage.
- Operational damage.

This determines the worst case credible effect on the node, taking into consideration single failure and ignoring safeguards already in place. This helps the analyst assess existing safeguards or propose additional safeguards if required.

7.3.2. Results. When the analysis phase is completed and all outstanding issues are resolved, the conclusions are prepared and a tabulation of recommended actions are prepared and submitted. Figure 7-3 shows a typical HAZOP worksheet. Sources of information typically include piping and hardware drawings, facility drawings, procedures, safety hazard analysis reports, and accident & investigation reports. The advantages of a HAZOP are that it is a very comprehensive hardware review, it is good for complex systems, and it provides very detailed results. The disadvantages of a HAZOP are that it is very time consuming, expensive, and may not pick up on multiple failures.

Guideword	Cause	Effect	Type	Safeguards	Recommen-dations	Actions
1	2	3 →	4 →	5 →	6 →	
	↓	7 →	8 →	9 →	10 →	
	↓					

HAZOP Worksheet
Figure 7-3

The HAZOP is not a quantitative assessment and consequence probabilities are not normally part of the analysis unless other quantitative techniques such as fault trees are integrated into the overall effort; however, the results of the analysis are directly proportional to the extent that the HAZOP team understands the process and has defined all of the process elements. As stated earlier, HAZOP is only one method of hazard evaluation. Other methods may be more suited to a facility assessment depending on the needs of the project.

7.4 SUBSYSTEM HAZARD ANALYSIS

7.4.1. Description. The Subsystem Hazard Analysis (SSHA) is performed to identify design hazards in subsystems. For a facility, subsystems could include an industrial laser, a computer controlled fire detection and suppression system, a vacuum chamber or special purpose test equipment. The requirement for a SSHA is usually identified in the concept phase of a system or facility. Due to the complexity of the analysis, the analysis is usually specified in a procurement specification then completed by the equipment/subsystem manufacturer.

The analysis should find functional failures of subsystems that could result in accidental loss. Component and equipment failures or faults, and human errors that establish a hazard due to the functioning of the subsystem are analyzed. The analysis is completed by reviewing design drawings, engineering schematics, and specifications.

The SSHA should be completed no later than the beginning of system definition phase of the system life cycle. As the system and related subsystems are further defined during system definition and development, the analysis should be revised. A sample sheet from a SSHA completed for a signal system is provided as Figure 7-4 (Roland and Moriarty, 1990).

ANALYSIS TYPE:: SUBSYSTEM HAZARD ANALYSIS							
SYSTEM SIGNAL SYSTEM PREPARED BY _____							
SUB-SYSTEM POWER DATE _____ SHEET _____ OF _____							
ITEM NO.	COM-PONENT	FUNCTION	HAZARD DESCRIPTION	HAZARD EFFECTS	HAZARD CATEGORY & PROB.	RECOMMENDED CONTROL	RESOLU-TION
1	AUTO-MATIC TRANS-FER SWITCH	AUTOMATICALLY PROVIDES POWER FROM EITHER NORMAL OR EMERGENCY SOURCE	AUTOMATIC TRANSFER SWITCH WILL NOT SHIFT FROM POWER SOURCE TO EMERGENCY POWER WHEN POWER SOURCE IS LOST	SIGNAL FAILS	1D	PROVIDE "VITAL" SIGNALS TO SHIFT ALL SIGNALS TO RED (STOP) CONDITION WHEN NO POWER IS AVAILABLE	
2	AUTO-MATIC TRANS-FER SWITCH	AUTOMATICALLY PROVIDES POWER FROM EITHER NORMAL OR EMERGENCY SOURCE	NO POWER IS AVAILABLE FROM EITHER NORMAL OR EMERGENCY POWER SOURCE	SIGNAL FAILS	1E	PROVIDE BACK UP BATTERY POWER	

Completed Signal System SSHA Form
Figure 7-4

7.4.2. Results. The SSHA identifies hazards to personnel, equipment, facilities, and program resources caused by loss of function, energy sources, hardware failures, personnel actions or inactions, software deficiencies, interaction of components, inherent design characteristics, incompatible materials, and environmental conditions (within the subsystem).

Results of an SSHA are referred to the managing activity for inclusion in the hazard analysis documentation. Unresolved hazards are listed in the HATI.

7.5 SYSTEM HAZARD ANALYSIS

7.5.1 Description. The System Hazard Analysis (SHA) examines the interfaces between subsystems. In so doing, it must integrate the outputs of the SSHA. It should identify safety problem areas of the total system design including safety critical human errors, and assess total system risk. Emphasis is placed on examining the interactions of the subsystems. The SHA should examine subsystem relationships for:

- Compliance with safety criteria specified in subsystem requirements documents.
- Sets of hazardous events, independent or dependent to include failures of safety devices and common cause conditions or events that can result in system or facility hazards.
- Degradation of safety of the overall system or facility from normal operation of a subsystem.
- Software control functions that may adversely affect system risk due to software faults.
- Human control functions that may affect risk through human faults.
- The SHA begins during the early design phases. The SHA is updated when interfaces are defined and continues on through to the beginning of system operation.

7.5.2 Results. Results of the SHA are presented in tabular form. Identified hazards which are not resolved are included in the HATI. Figure 7-5 shows the results of a SHA for a tunnel pumping system.

7.6 OPERATING AND SUPPORT HAZARD ANALYSIS

7.6.1. Description. Most safety analyses are directed towards uncovering design problems associated with hardware. This is not the intent of an Operating and Support Hazard Analysis (O&SHA). The purpose of the O&SHA is to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element. The O&SHA identifies, documents, and evaluates hazards resulting from the implementation of operations or tasks performed by persons and considers:

- The planned system configuration at each phase of activity,
- The facility interfaces,

ANALYSIS TYPE:: SYSTEM HAZARD ANALYSIS

SYSTEM PUMPING SYSTEM PREPARED BY _____

SUB-SYSTEM PUMP, CONTROLLER POWER DATE _____ SHEET _____ OF _____

ITEM NO.	COM-PONENT	FUNCTION	HAZARD DESCRIPTION	HAZARD EFFECTS	HAZARD CATEGORY & PROB.	RECOMMENDED CONTROL	RESOLU-TION
1	POWER CABLE	TRANSFERS POWER BETWEEN SOURCE AND PUMP	PUMP CONTROLLER POWER CABLE FAILS - LACK OF POWER	LOSS OF PUMPING CAPABILITY - WATER FLOODS TUNNEL	1D	PROVIDE REDUNDANT POWER CABLE	
2	PUMP CON-TROLLER	PROVIDES CONTROL OF PUMP OPERATION	PUMP REMAINS ON CONTINUOUSLY - PUMP BURNS OUT	WATER FLOODS TUNNEL	1B	PROVIDE LOW WATER CUT-OFF FOR PUMP	

Completed Tunnel Pumping System SHA Form
Figure 7-5

- The planned environments, the support tools, or other equipment specified for use,
- Operation or task sequence,
- Concurrent task effects and limitations,
- Biotechnological factors,
- Regulatory or contractually specified personnel safety and health requirements, and
- The potential for unplanned events including hazards introduced by human error.

The O&SHA identifies the safety requirements (or alternatives) needed to eliminate identified hazards, or to reduce the associated risk to a level which is acceptable.

To perform an O&SHA, pertinent data such as procedures, sequence diagrams, operation and functional analyses, equipment layout diagrams, systems and subsystem design specifications, equipment and interface drawings, operations and maintenance instructions, and human factors engineering data should be obtained if available. A worksheet is commonly used to develop the hazards. It is similar to the FHA but with an operational event as the primary categorizing function. Operational events are sets of sequenced actions for operating, assembling, maintaining, repairing, calibrating, testing, transporting, handling, installing, or removing an assembly, component, or system. These events are generally documented in procedures. An analysis of the procedures is completed to ensure that:

- Required tasks, human-machine-environment and interpersonal relationships, and the sequences of operational steps will not lead to a mishap.
- Completing the procedure does not expose personnel to any hazards.
- Instructions are clear and effective and do not induce errors that could lead to mishaps.
- Alternative actions a person could take which could result in mishaps are precluded, or the effects of such actions are minimized.
- Safety-critical steps are highlighted with warnings and cautions.
- No extraordinary mental or physical demands are made for programmed operations.
- Times for accomplishment of safety-critical tasks are realistic.

The following should also be accomplished to ensure the procedures are safe:

- Examine the procedure and each step within the procedure for effect, necessity, and clarity. Personnel tend to take shortcuts in order to avoid arduous, lengthy, uncomfortable, or ambiguous procedures. The shortcuts can sometimes lead to errors and mishaps.
- Examine each procedure and each step, no matter how simple it appears, for possibilities of error, alternative actions, and adverse results.
- Determine whether or not special training, knowledge, or capability is required which the prospective operator might not have.
- Review the causes of error and attempt to eliminate or minimize the possibilities of as many of them as possible.
- Verify the proposed procedures by examining, demonstrating, and testing.

After the operating procedures are analyzed, the procedures should be verified. This verification should be done by persons not involved in writing or analyzing the procedures. A checklist should be used to assist in verifying the procedures. In addition, the analyst should try to perform the procedures as prescribed by the author of the procedures and then try to anticipate any alternative actions the user might take. The person performing the procedures should verify that safeguards will work as intended, that emergency stop systems can be reached and will stop an operation when they are supposed to, that detection and warning devices operate, that personnel protective equipment can be reached and donned within planned lengths of time, and that emergency routes and exits are practical.

7.6.2. Results. An O&SHA is very useful and can give valuable information, such as:

- Corrective or preventive measures that should be taken in order to minimize the possibilities of an error resulting in a mishap.

- Recommendations for changes or improvements in hardware or procedures in order to improve efficiency and safety.
- Development of warning and caution notes to be included in the most effective places in the procedures.
- Requirements for special information or training of personnel who will carry out the procedures.
- Recommendations for special equipment, such as personnel protective clothing or devices, which would be required for the operations to be undertaken.

Figure 7-6 shows the results of an O&SHA worksheet.

OPERATING & SUPPORT HAZARD ANALYSIS BATTERY BOX

STATION: Technician DATE: _____

OPERATIONAL MODE: Run SHEET NO: ____ OF ____

ID #	Process/Task	Hazardous Condition	Cause	Effect	Hazard Category	Hazard Probability	Status/ Recommendation
1.	Connecting/disconnecting emergency lights to sealed connections on battery box.	Water enters into connector	Connectors cracked or seal is defective.	Electrical shock to personnel.	1-Catastrophic	B- Possible	Daily inspection of connectors; Replace when deficiencies are detected.
2.	Removal and replacement of battery box.	Fall on personnel. Fall on equipment.	Lifting lugs fail. Nylon webbing fails.	Injury to personnel. Damage to equipment.	1-Catastrophic	B- Possible	A. Assure integrity of weld lugs. B. Perform regular inspections of webbing; Replace when frayed or worn. C. Train personnel in safe raising/lowering box. D. Train personnel to stand clear when box is being raised or lowered.

Example O&SHA Worksheet
Figure 7-6

7.7 FAULT TREE ANALYSIS

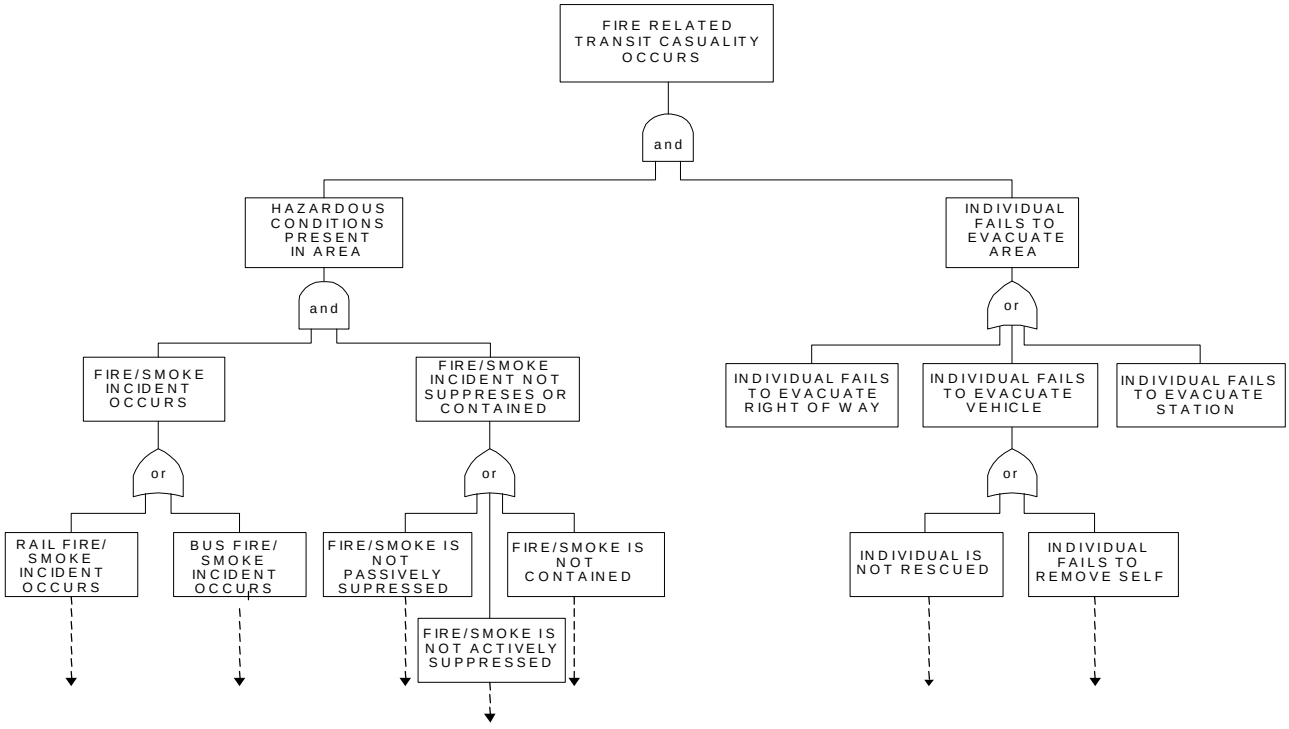
7.7.1. Description. A fault tree analysis (FTA) can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with

component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event which is the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes of system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive, they cover only the most credible faults assessed by the analyst.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively and often is. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself.

A fault tree is a complex of entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationship of events needed for the occurrence of a "higher" event which is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event. Thus, gates are somewhat analogous to switches in an electrical circuit or two valves in a piping layout. Figure 7-7 shows an example fault tree.



Example Fault Tree
Figure 7-7

7.7.2. Results The output of a FTA is a graphic functional failure representative of the system or facility. Though the FTA itself is qualitative, quantitative data can be annotated to the tree in the form of event or component failure probabilities, thus quantifying the FTA.

7.8 FAILURE MODE AND EFFECTS ANALYSIS

7.8.1. Description. The Failure Mode and Effects Analysis (FMEA) is a reliability analysis. The focus of the analysis is on single events or component failures that will cause a state of unreliability in the system (Roland and Moriarty, 1990). The objective of the FMEA is to view each identifiable component in the system in the context of two questions:

- How can the component fail?
- What will be the results of this failure downstream in the system or subsystem?

This effort can improve knowledge of potential component, subsystem, or system failures that were found by the FHA. The FMEA is used to methodically track each component's major failure effects into other subsystems and to develop an understanding of the hazardous impact on one component's failure on the rest of the system. As with the SSHA, this analysis methodology requires in-depth knowledge of the system, and is generally specified in a procurement specification and then completed by the system or equipment manufacturer.

FMEA analysis is conducted by asking each of the two above cited questions in relation to components and then projecting the likely physical and functional effects of the failures on other parts of the system. Effects of failure are stated in terms of associated damage or malfunction accompanied by qualitative assessments of frequency and severity suitable for Hazard Risk Indicator (HRI) ranking.

7.8.2. Results. The FMEA output is a columnar worksheet shown such as the one in Figure 7-8. An HRI code for each item may be substituted for the “Probability of Failure". One of the strengths of FMEA is that it promotes identification of problems associated with the interface of subsystems and/or components. Using the specified output format, detected hazards will be described for characteristics and recommended control action(s). Though the FMEA is qualitative, failure probabilities can be included for decision making purpose.

7.9 SOFTWARE HAZARD ANALYSIS

7.9.1. Description. The traditional approach to the hazard analysis of complex electromechanical systems is to treat electronic devices that process or originate system control signal as black boxes. This approach precludes analysis of the internal functioning of the box. Output reliability of the box is established relative to input and this value inserted into the system model as a quantitative representation of a pseudo-mechanical component of the system. When we replace the box with a small computer, processing instructions that have been permanently installed in the memory, we have quite another situation. If the software containing the

			FAILURE EFFECT ON			
COMPONENT NAME AND NUMBER	FUNCTION	FAILURE MODE AND CAUSE	NEXT HIGHER ASSEMBLY	END ITEM PRODUCT	PROBABILITY OF FAILURE (Σ X 10^{-6})	CORRECTIVE ACTION AVAILABLE OR RECOMMENDED
Cover Cap	Keeps coffee from being thrown about: keep user from getting fingers into cap where they could be cut by rotor.	Plastic fractures and parts separate. Brittle plastic dropped on hard surfaces, stepped on, or subjected to excessive force when being put in place.	None	None	1	Select plastic which is not brittle.
Switch Activating arm (1)	User depresses and holds down free end in access hole to switch which operates mill.	Breaks off cap due to rough handling by user,. being stepped on, or dropped.	May cause cap to weaken and break if arm breaks off in cap.	May make product unusable.	100	Redesign. Put switch under cap, thereby eliminating area.
Case Case, plastic (1)	Major structural part which holds other assemblies together: protects against contact with moving and electrical parts.	Could be broken by impact or crushing.		Resultant sharp edges and points; may make it unusable.	0.5	Use impact resistant plastic.
Vibration dampers (2)	Brittle pads in case. Reduction of vibration and noise by separating metal motor frame from plastic case.	Deterioration of rubber. Could be lost since they are not glued in place.	Fatigue to brittle plastic.	Excessive vibration and noise.	0.01	Glue in place.

Example Failure Modes and Effects Analysis
Figure 7-8

instructions is error or fault free, then this component cannot fail and the statistical concept of measuring stochastic wearouts has no meaning. However, the software instructions may contain faults. This possibility will require an analysis of the computer program code that has become instructions to the hardware system (Roland and Moriarty, 1990).

Control systems and control computers are usually in a high state of flux. Both hardware and software need to be analyzed for all faults and failures, including using probabilistic risk assessment techniques. Because of potentially frequent changes, which are relatively easy to make compared to hardware changes, control systems and software need to be under strict change control, as per the Center configuration management plan. Software is coded by programmers working to a specification set forth by system designers. Software faults may take three forms.

- The so-called honest errors made by the programmer in coding the software specification. These are simple mistakes in the coding process that result in the software behaving in a manner other than that which the programmer intended.

- Faults due to incorrect software specifications or the programmer's interpretation of these specifications. These errors may result from system designer's lack of full understanding of system function or from the programmer's failure to fully comprehend the manner in which the software will be implemented or the instructions executed. In this type of fault the software statements are written as intended by the programmer.

- Faults due to hardware failure. Hardware failures may change software coding. Thus such software faults are secondary in that they originate outside the software.

A software hazard may be one of the following four types:

- An undesired signal causes an unwanted event in the system functional process.

- An undesired signal causes an out-of-sequence event.

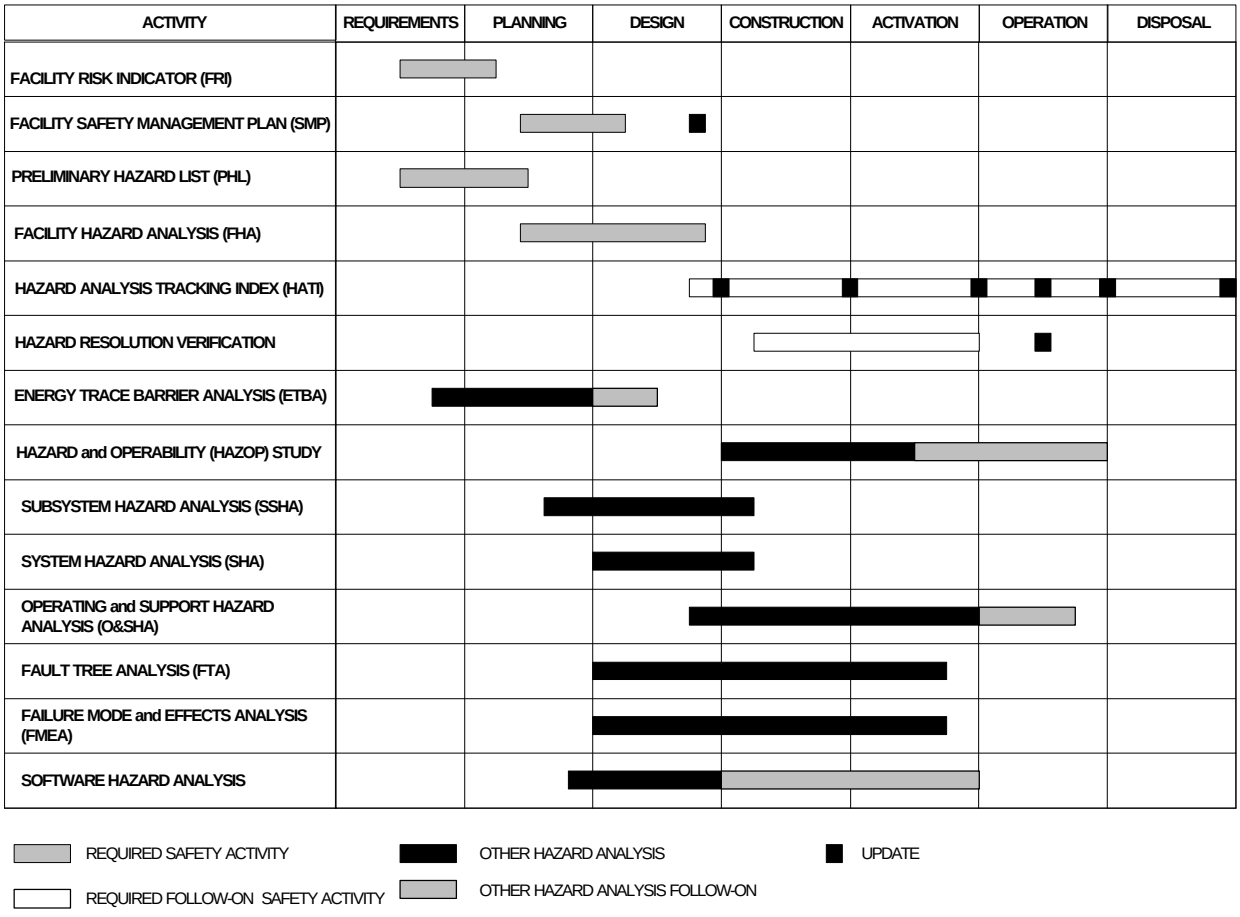
- An undesired signal prevents the occurrence of a needed event.

- An undesired signal causes an event that in magnitude or direction is out of tolerance.

7.9.2. Results. The results of the software analysis are as varied as the analyses themselves. Usually the data results are presented in tabular form. Graphs can also be used to depict causal relationships.

7.10 HAZARD ANALYSIS SCHEDULES

Figure 7-9 indicates the most appropriate time that the various hazard analyses can be performed throughout the facility life cycle. Obviously, many of them overlap during the facility life cycle.



Facility System Safety Milestone Activities
Figure 7-9

APPENDIX A
TYPICAL ENERGY SOURCES CHECKLIST

A. Acoustical Radiation

Equipment Noise
Ultrasonic Cleaners
Compressors

B. Corrosive

Acids
Caustics
Natural Chemicals (Soil, Air, Water)
Decontamination Solutions

C. Electrical

Battery Banks
Diesel Units
High Lines
Transformers
Wiring
Switchgear
Underground Wiring
Cable Runs
Service Outlets and Fittings
Pumps
Motors
Heaters
High Voltage Sources
Electrostatic Sources (low humidity)

D. Electromagnetic and Particulate Radiation

Radioactive Sources
Waste and Scrap
Contamination
Irradiated Experimental and Reactor Equipment
Electric Furnace
Blacklight (e.g., Magniflux)
Laser
Medical X-ray
Radiography Equipment & Sources
Welding
Electric Arc - Other (High Current Circuits)
Electron Beam
Radar
Alternating Current (AC) Motors

E. Explosive Pyrophoric

Caps
Primer Cord
Dynamite
Power Metallurgy
Dusts
Hydrogen (Inc. Battery Banks and Water Electrolysis)
Gases-Other
Nitrates
Electric Squibs
Peroxides-Superoxides
Propellant

F. Thermal (Except Radiant)

Convection
Heavy Metal Weld Preheat
Exposed Steam Pipes
Electric Heaters
Fire Boxes
Lead Melting Pot
Electrical Wiring & Equipment
Furnaces

G. Flammable Materials

Packing Materials
Rags
Gasoline (Storage & in Vehicles)
Lubrication Oil
Coolant Oil
Paint Solvent
Diesel Fuel
Buildings and Contents
Trailers and Contents
Grease
Hydrogen (Including Battery Banks)
Gases - Other
Spray Paint
Solvent Vats

H. Kinetic-Linear

Cars
Trucks
Buses
Fork Lifts
Carts
Dollies
Trains
Surfaces
Obstructions
Shears
Presses
Crane Loads in Motion
Pressure Vessel Blowdown
Power Assisted Driving Tools
Monorails

I. Mass, Gravity, Height

Human Efforts
Stairs
Lifts
Cranes
Buckets and Ladders
Trucks
Slings
Hoists
Elevators
Jacks
Scaffolds and Ladders
Crane Cabs
Pits
Excavated Doors
Elevated Doors
Canals
Vessels

J. Kinetic-Rotational

Centrifuges
Motors
Pumps
Cooling Tower Fans
Cafeteria Equipment
Laundry Equipment
Gears
Shop Equipment (Grinders, Saws, Brushes, etc.)
Floor Polishers

K. Pressure-Volume/K-Constant-Distance

Test Loops and Facilities
Gas Bottles
Pressure Vessels
Coiled Springs
Stressed Members
Gas Receivers

L. Thermal Radiation

Furnaces
Boilers
Steam Lines
Laboratory and Pilot Plant Equipment
Solar
Boilers
Heated Surge Tanks
Autoclaves

M. Toxic Pathogenic

Acetone
Fluorides
Carbon Monoxide
Lead
Ammonia and Compounds
Asbestos
Trichlorethylene
Dusts and Particulate
Pesticides-Herbicides-Insecticides
Bacteria
Beryllium and Compounds
Chlorine and Compounds
Decontamination Solutions
Sandblasting Operations
Metal Plating
Asphyxiation-Drowning

N. Nuclear

Vaults
Temporary Storage Areas
Receiving Areas
Shipping Areas
Casks
Burial Ground
Storage Racks
Canals in-Tank Storage Areas
Dollies
Trucks
Hand Carry
Cranes
Lifts
Commercial
Shops
Hot Cells
Assembly Areas
Inspection Areas
Test Rigs
Reactors
Critical Facilities
Subcritical Facilities
Laboratories
Pilot Plants

APPENDIX B
PRELIMINARY HAZARD LIST EXAMPLE
GENERAL LABORATORY FACILITY

AREAS OF CONCERN/SAFETY CONSIDERATIONS

(1) Building Materials
- Compatibility
- Flammability
- Structural integrity

(2) Access/Egress
- Emergency - evacuation, fire fighting, rescue
- Panic hardware
- Restricted - security, clean rooms
- Handicapped/disabled
- Operations and maintenance
- Inspection
- Life safety code requirements

(3) Utilities
- Location
- Controls/shutoffs
- Electrical power supply
- Water supply
- Sanitary/sewer
- Natural gas
- Special systems - bulk gas

(4) Ventilation
- Heating
- Air conditioning
- Clean room environment
- Filters/dust control
- Humidity control
- General exhaust
- Emergency
- Recirculation/migration/reentrainment

(5) Electrical
- Emergency power
- Electrostatic discharge

(5) Electrical (Continued)
- Shock
- Wiring
- Switchgear
- Shutoffs/breakers
- Wires/cables under raised floor
- Intra- and inter-room cable management/computer networks
- Grounding/bonding
- Insulation
- Cathodic protection
- Lasers - high energy power supply, capacitors, interlocks
- Lock-out / tag-out

(6) Lighting
- Ambient
- Emergency
- Exit
- Security

(7) Fire Protection
- Fire/smoke detection
- Pull stations
- Alarms/annunciation
- Automatic fire suppression
- Extinguisher selection/location
- Standpipe hose connections
- Siamese connections
- Hydrants
- Smoke management
- Fire resistive construction
- Fire barrier design/construction
- Compartmentalization / isolation from different occupancies
- Fire department access

(8) Monitoring
- System/utility - pressure, temperature, flow, voltage, grounds
- Environmental - air quality, temperature, humidity
- Security
- Fire/smoke detection
- Hazardous gas/vapor detection
- Leak detection
- Alarms/annunciation

(9) Communications
- Public address
- Emergency - fire department, police, medical services
- Alarms/central station

(10) General
- Stairs/railings
- Traffic
- Sidewalks
- Loading/unloading
- Trailer pads
- Height - rooftop observation dome, roof mounted antennae

(11) Natural Phenomena
- High wind
- Snow
- Extreme temperatures
- Floods
- Lightning
- Earthquake

(12) Kinetic/Mechanical
- Sparks/friction
- Overhead cranes
- Machine guards
- Power tools
- Elevators
- Overhead doors
- Staging

(13) Pressure
- Hydraulics
- Compressed gases - bottles, tanks
- Air/pneumatic systems
- Relief valves
- Steam
- Pumps

(14) Confined Space
- Vacuum chambers
- Raised floors
- Utility tunnel

(15) Laboratory Design
- Benches/work surfaces
- Storage
- Drainage
- Exhaust/ventilation
- Clean room environment
- Utilities
- Space utilization/placement
- Cross connection/backflow prevention

(16) Radiation
- Ionizing - alpha particles, beta particles, neutrons, x-rays, gamma rays
- Electromagnetic - lasers, radar, ultraviolet (UV) and infrared (IR) light, microwaves, radio frequency (RF) waves, high frequency signals from computer equipment
- Acoustical - laboratory and ventilation equipment noise
- Thermal

(17) Hazardous Materials
- Flammables/combustibles
- Explosives/pyrophorics
- Toxic substances/poisons
- Corrosives
- Oxidizers
- Water reactive/unstable substances
- Irritants
- Asphyxiants
- Radioactive materials
- Carcinogens/pathogens

(18) Material Handling
- Storage - quantity, location, isolation/fire control areas, compatibility, inventory control
- Transfer/delivery
- Use
- Disposal
- Spill control
- Containment
- Exhaust/ventilation

(19) Environmental
- Resource Conservation and Recovery Act (RCRA) considerations
- Hazardous waste
- Hazardous spill/release

- Exposure to environment
- Exposure from environment

(20) Exhaust
- General
- Local
- Fume hoods
- Emergency
- Scrubber/filtration
- Recirculation/migration/reentrainment

(21) Personnel Safety
- Personal protective equipment - gloves, gowns, eye and ear protection, respirators
- Eyewashes/showers
- Graphics
- Thermal contact - burns (hot and cold)
- Exposure control
- First aid
- Pre-action alarms for carbon dioxide/nitrogen extinguishing systems

(22) Documentation
- Material Safety Data Sheets (MSDS)
- Training
- Emergency action plan
- System safety plan
- Operating procedures
- Maintenance procedures
- Test procedures
- Chemical hygiene plan
- Configuration control plan

(23) Operations
- Electronic/mechanical testing and analysis
- Cooking/kitchen equipment
- Spectroscopy/optics
- Chromatography
- Magnetic analysis
- Cryogenics
- Fabrication/machine shop
- Lasers
- Supercomputer operations

APPENDIX C

EXAMPLE
FACILITY SAFETY MANAGEMENT PLAN
GENERAL LABORATORY FACILITY

TABLE OF CONTENTS

EXAMPLE
FACILITY SAFETY MANAGEMENT PLAN
GENERAL LABORATORY FACILITY

TABLE OF CONTENTS (CONTINUED)

APPENDIX D

EXAMPLE FACILITY HAZARD ANALYSIS

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Fire Protection
Subsystem: Building Design and Construction

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
1.1.01	Fire spreading through buildings or structures.	Materials selected during design or construction are not fire-rated or are combustible.	Contribute to fire spreading possibly causing injury and equipment and facility damage.	IC	Select construction materials in accordance with industry standards for fire prevention. Shall not use combustible materials in building construction for a non-combustible building. Follow requirements for a UBC type I fire-resistive building.	IE	3	1	UBC Ch. 18;UBC Ch. 17;UBC Ch. 5	Closed
1.1.02	Excess storage of hazardous materials. Quantities of hazardous materials for a control area exceeds those listed in UBC Tables No. 9-a or 9-b.	Design does not consider the quantities nor types of hazardous materials during laboratory layout and control area definitions.	Personnel injury or illness from hazardous materials.	IIB	Review overall, control area, and individual laboratory unit quantities and types of hazardous materials, liquids and chemicals presenting a physical or health hazard. Ensure maximum quantities per control area do not exceed UBC tables 9-a or 9-b.	IIE	3	1	UBC 702(c)3.;UBC Ch.9	Closed
1.1.03	Excess storage of hazardous materials. Quantities of hazardous materials for a control area exceeds those listed in UBC Tables No. 9-a or 9-b.	Increased quantities of hazardous materials during continued operations may change the hazard level of the facility.	Personnel injury or illness from hazardous materials.	IIB	Periodically the quantities of chemicals that are used and stored in the entire facility and per control area, especially if operations change. Ensure that adequate safety precautions are taken if occupancy classification changes.	IIE	3	1	UBC 702(c)3.;UBC Ch.9	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Fire Protection
Subsystem: Fire Suppression

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
1.2.01	Failure to automatically suppress fire.	Automatic fire suppression system not present.	Fire/explosion. Unchecked fire growth causes increased property damage and risk to personnel, including firefighters.	IC	NSS 1740.11 Ch. 502(a) States, “Automatic prinkler protection shall be provided for all COF Funded building/facility construction.” The spinkler system should be a wet pipe system. Design in accordance with applicabel codes.	IE	3	1	NSS 1740.11 Ch. 502(a);NFPA 13, NFPA 25;OSHA 1910.159	Closed
1.2.02	Automatic sprinkler system malfunctioning. Failure to automatically suppress fire.	The automatic fire suppression system did not have a system acceptance prior to facility operations.	Fire. Unchecked fire growth causes increased property damage and risk to personnel, including firefighters.	IC	The installing sprinkler contractor shall: (a) notify the authority having jurisdiction and owner's representative of the time and date testing will be performed. (b) perform all required acceptance tests of NFPA 13 ch. 8.;(c) complete and sign the inspection forms.	IE	3	1	NFPA 13 Ch. 8;OSHA 1910.159(c)(3)	Open
1.2.03	Water-based fire protection system is not operating properly. Failure to automatically suppress fire.	Automatic fire suppression system not inspected, tested, and maintained properly (after facility acceptance).	Fire/explosion. Unchecked fire growth causes increased property damage and risk to personnel, including firefighters.	IC	The water-based fire protection system shall be properly inspected, tested, and maintained in accordance with NFPA 25 to met the original design specifications. Gsfc shall be responsible for maintaining the system and keeping the system in good operating	IE	3	1	NSS 1740.11 Ch. 502(i);NFPA 25, NFPA 13 Ch. 9;OSHA 1910.159(c)(2)	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Fire Protection
Subsystem: Fire Department Operations

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
1.3.01	Fire/explosion (fire service problems).	Lack of adequate access (by fire department and emergency responders) to facility hinders fire suppression activities.	Creates fire damage and injuries. Also subject fire service personnel to unnecessarily hazardous working conditions.	IB	Provide adequate fire service access (by fire department and emergency responders) to facility in order to allow for rapid response to fire and to ease individual threats of injury. Provide well marked fire lanes.	IE	3	1	UFC Article 10 Div. II and Div. III;Prince George's County Fire Department	Closed
1.3.02	Fire spreading.	Design does not consider the adequate number and placement of working standpipe connections.	Catastrophic personnel injury or possible death, or loss of equipment or system, due to loss of control of fire due to inadequate or unavailable standpipe connections.	IC	Provide adequate number of well placed standpipe connections for fire department connection during a fire. A standpipe shall be located 1) at every floor of every required exit stairway, 2) at the highest landing of stairways with stairway access to the roof.	IE	3	1	NFPA 14 specifically Ch. 5-3.2;UBC 3805;UFC 10.510	Closed

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Fire Protection
Subsystem: Detection, Alarm, Monitoring, and Communications

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
1.4.01	Undetected fire. Personnel, emergency responders, and fire department unaware of fire/ emergency.	Inadequate or lack of fire detection alarm/ system.	Unchecked spread of fire. Personnel injury and equipment loss.	IC	Ensure adequate fire detection, alarm, and communications systems are designed / incorporated into fire protection system.	IE	3	1	NSS 1740.11 Par. 603-604;NFPA 72;NFPA 101 Ch. 7-6;NFPA 101 Ch. 26-3.4;OSHA 1910.164-165;UFC Article 14	Closed
1.4.02	Personnel not adequately alerted of fire/ emergency.	Inadequate or lack of fire alarms for occupant notification.	Personnel not escaping from area/ building. Personnel injury.	IC	Occupant notification shall provide signal notification to alert occupants of fire or other emergency. Alarms should be both audible and visible, and adequately located.	IE	3	1	NFPA 101 Ch. 7-6.3;NFPA 101 Ch. 26-3.4.3;NFPA 72 Ch. 6;OSHA 1910.165;UFC 14	Closed
1.4.03	Personnel not adequately alerted of emergency situation.	Warnings and alarms, such as fire alarm bells/buzzers, not loud or noticeable enough for all personnel in all operating conditions.	Personnel injury or death, equipment damage or loss.	IC	Ensure that all operating scenarios, including personnel location and ambient noise levels, are considered in designing layout/location, loudness, etc. Of alarm systems, including fire alarms. Ensure audible alarm can be effectively heard.	IE	3	1	NFPA 72 Ch. 6-3;NSS 1740.11 Par. 603(k)(2);NSS 1740.11 Par. 603(f)	Closed

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Exposure Control
Subsystem: Ventilation

Date: July 11, 1997
Page: 22
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
2.1.01	Entrainment of contaminated exhaust air by facility fresh air intakes.	Improper location of outside fresh air intakes.	Unpleasant odors, potentially acute and systemic toxic health effects to building occupants.	IIB	Locate outside fresh air intakes to avoid drawing in hazardous chemicals, combustion material, or flammable vapors, and to minimize hazard from fires coming from either the building itself or from other structures.	IIE	3	1	NFPA 90A Sec. 2-2.1;NFPA 45 Ch. 6-4.1;ASHRAE HANDBOOK-1989-Fundamentals Ch. 14 "Airflow Around Buildings", ACGIH Industrial Ventilation, 21st edition Ch. 5	Closed
2.1.02	Accumulation of indoor air contaminants.	Inadequate supply of fresh outdoor air.	Feeling of "stuffiness", unpleasant odors, potentially acute and systemic toxic health effects for personnel, affecting morale and productivity.	IIIC	Design system to provide outdoor air to meet minimum requirements of ansi/ashrae standard 62-1989.	IIIE	3	2	ASHRAE Standard 62-1989	Closed
2.1.03	Fire spreading rapidly through HVAC ducts within building.	Unsafe fire protection in construction materials for HVAC duct work.	Contribute to fire spreading possibly causing injury or death and equipment and facility damage.	IC	Hvac ducts and plenums should be constructed entirely of noncombustible, nonporous materials (ul standard 181). Their construction should comply with NFPA and other industry standards.	IE	3	1	NFPA 90A;UL Standard 181	Closed

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Exposure Control
Subsystem: Exhaust

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
2.2.01	Entrainment or reentry of contaminated exhaust air or hazardous chemicals into the building.	Improper design of discharge stacks and exhaust system.	Unpleasant odors, potentially acute and systemic toxic health effects to building occupants.	IIB	Exhaust air shall be discharged above the roof at a location, height, and velocity sufficient to prevent reentry of hazardous chemicals. Design stacks to extend above the eddy zone. Mushroom exhaust fans are not permissible for local exhaust systems.	IIE	3	1	NFPA 45 Sections 6-4.1 & 6-8.7;NFPA 91 Sec. 2-11;ASHRAE Handbook-1989-FundamentalS Ch. 14 "Airflow Around Buildings", ASHRAE Handbook-1991-HVAC Applications Ch. 14 "Laboratories";ACGIH Industrial Ventilation, 21st Edition Ch. 5	Closed
2.2.02	Contamination of air immediately outside facility	Exhaust of toxic gases/fumes at too low level near facility	Environmental contamination, personnel injury or illness to persons on roof or near the facility.	IIB	Ensure that exhaust stacks from facility are at sufficient heights to avoid contamination of atmosphere around facility in regards to personnel.	IIE	3	1	ASHRAE Handbook-1989-Fundamentals, Ch. 14;NFPA 45 A. 6-8.7;ACGIH Industrial Ventilation, 21st Edition	Closed
2.2.03	Contamination of air immediately outside facility.	Exhaust of toxic gases/fumes at low level on roof or near the facility.	Environmental contamination, personnel injury or illness to persons on roof or near the facility.	IIB	Periodically test the roof and area surrounding the facility for possible air contamination, and to ensure that exhaust stacks are at sufficient heights. Perform tests when utilizing new hazardous materials.	IIE	3	1	ASHRAE Handbook-1989-Fundamentals, Ch. 14	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Exposure Control
Subsystem: Personnel Safety

Date: July 11, 1997
Page: 32
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
2.3.01	Prolonged effect of chemical burns, eye damage, contaminated personnel.	Failure to provide equipment needed to decontaminate personnel handling hazardous materials/waste that may have come in contact with eyes, clothing or skin. Lack of or no eyewashes / emergency showers.	Personnel injury including loss of eye sight and burns from exposure to strong acids and bases.	IIB	Provide eyewash and overhead deluge emergency stations (showers) within 25 feet or 15 seconds travel time from the hazard or work station. Units should be easy to locate and in the path of normal egress.	IIE	3	1	ANSI Z358.1;OSHA 1910.151(c);NSC DATA SHEET 1-686-80	Open
2.3.02	Prolonged effect of chemical burns, gas fumes in eyes.	Inadequate types, water supply, and controls of eyewashes and emergency showers.	Personnel injury.	IIC	Provide adequate types, water supply, and controls of eyewashes and emergency showers.	IIE	3	2	NSC DATA SHEET 1-686-80	Closed
2.3.03	Prolonged effect of chemical burns, gas fumes in eyes.	Personnel are not trained to operate eyewashes and emergency showers. System not functioning properly.	Personnel injury.	IIC	Provide adequate training for eyewashes and emergency showers. Periodically test eyewashes and emergency showers for their correct operations.	IIE	3	2	NSC DATA SHEET 1-686-80	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Exposure Control
Subsystem: Hazardous Materials

Date: July 11, 1997
Page: 39
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
2.4.01	High hydrogen concentration leads to a fire or personnel asphyxiation.	Lack of hydrogen gas detection devices in facility.	Personnel death, fire, or explosion.	ID	Provide hydrogen gas detectors in laboratory areas which store and use hydrogen gas. Provide emergency power to the gas detection system. The alarm should sound both locally and in the emergency console in building 24.	IE	3	2		Closed
2.4.02	Release of toxic or highly toxic gases.	Lack of means to detect toxic and highly toxic gases in facility.	Personnel death or illness.	IIA	Provide a continuous gas detections system to detect the presence of gas at or below the permissible exposure limit or ceiling limit in laboratory areas which store and use toxic and highly toxic gases. See appendix a for listing of gases and locations.	IIE	3	1	UFC 80.303(a)(9);UFC 80.303(a)(7)	Open
2.4.03	Undetected build-up of hydrogen gas and/or toxic gases.	Gas detection system inoperable due to failure to accurately calibrate gas detectors and system.	Fire/ explosion. Personnel death or illness.	IB	Provide accurate calibration of all gas detectors and system.	IE	3	1		Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Exposure Control
Subsystem: Radiation

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
2.5.01	Non-ionizing radiation.	Radio frequency, infrared, ultraviolet radiation associated with processing equipment operation.	Health effects to personnel performing maintenance or operations.	IIB	Design equipment installation protocols to verify equipment radiation systems integrity. Establish safety protocols for maintenance and operation of equipment and systems.	IIE	3	1	OSHA 1910.97	Open
2.5.02	RF(radio-frequency), emr (electromagnetic radiation) or other non-ionizing radiation.	Equipment in laboratories emitting non-ionizing radiation.	Personnel injury due to non-ionizing radiation effects.	IIIB	Ensure that all equipment in laboratories which emit non-ionizing radiation are shielded to prevent harmful emissions. Personnel must use necessary protection. Ensure that equipment and laboratories are properly labeled for all hazards.	IIID	3	2	OSHA 1910.97	Open
2.5.03	High noise level in work areas.	Excessive equipment noise.	Personnel may receive wrong instructions causing increased chance of accident. Communication during emergency may be hampered.	IIC	Keep the lowest possible noise emission level in all work areas and in accordance with nasa and osha recommendations.	IIE	3	2	NHS 1845.4;OSHA 1910.95;OSHA 3048 - "Noise Control, A Guide For Workers And Employers"	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Storage

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.1.01	Increased risk of fire, explosion, and/or generation of toxic gases.	Accidental mixing of reactive materials with incompatible substances such as water, corrosive, toxic, or flammable materials, or other reactive substances, due to improper storage of reactive chemicals.	Personnel injury or death, and property loss may occur.	IC	Provide physically separate storage areas (rooms) for incompatible materials. Numerous storage areas may be required depending on the number and types of reactive chemicals stored. The hazards of each reactive material must be carefully reviewed for proper storage conditions.	IE	3	1	UBC Ch. 9;NFPA 30, NFPA 45;OSHA 1910.106;UFC 79;UFC 80	Closed
3.1.02	Increased risk of fire, from the improper storage of reactive materials.	Accidental mixing of reactive materials, such as: toxics or corrosives, flammables, etc.) With incompatible chemicals.	Personnel injury or death and property loss may occur.	IC	Provide separate chemical storage cabinets for incompatible materials. Numerous cabinets may be required depending on the number and types of reactive chemicals stored. Provide cabinets for flammable materials and other cabinets for other hazardous materials. Provide raised sills or spill trays in cabinets for spill protection.	IE	3	1	NFPA 30, NFPA 45;UFC 79, UFC 80;OSHA 1910.106	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Transfer, Delivery, and Movement

Date: July 11, 1997
Page: 47
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.2.01	Build-up of static electricity.	Measures for prevention of static charge build-up are inadequate or nonexistent for chemical transfer operations.	Explosion/fire. Personnel injury/death. Equipment and facility damage/loss.	IB	Dissipation of charge is accomplished by grounding container through a closed connection (contact is made before flow starts and is broken after flow is completed).	IE	3	1	NFPA 77 CH. 4-4	Open
3.2.02	Open container knocked over, causes liquid chemical spill.	Improper container storage.	Fire/explosion, property damage, personnel injury, death.	IB	Provide proper transfer equipment that supports containers. Prevent unsupported open containers.	ID	2	1	OSHA 1910.106;OSHA 1910.176;NFPA 45	Open
3.2.03	Fire/explosion.	Vapors created during transfer operations. Leak in transfer piping/equipment.	Property damage, personnel injury, death.	IB	Provide proper equipment and training for proper transfer operations. Provide maintenance program for all transfer equipment. Follow manufacturers' specifications.	ID	2	1	OSHA 1910.106;NFPA 30	Open
3.2.04	Overflow of chemical during transfer.	Improper transfer procedures and/or equipment. Untrained personnel performing transfer operations.	Fire/explosion, property damage, personnel injury, death.	IB	Use only approved transfer equipment with safety features. Establish appropriate procedures and training. Provide vent line for liquid nitrogen (ln2) transfer.	ID	2	1	OSHA 1910.106;NFPA 30;UFC	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Spills and Leaks

Date: July 11, 1997
Page: 50
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.3.01	Wet floor creates dangerous operating conditions.	Water/fluid releases from equipment. Improper drainage design for spills.	Personnel injury due to shocks (if electrical equipment present) or slips and falls.	IIA	Ensure that equipment design has own spill containment. Ensure proper drainage design to facilitate clean-up of water/fluid spills.	IIE	3	1		Open
3.3.02	Slippery floors on walkways or in working areas.	Smooth, slick floors. Spilling of fluids including cleaning solutions onto walkways and working surfaces.	Personnel injury due to slips and falls or electrical shocks if electrical equipment is present.	IIIA	Ensure that procedures facilitate clean-up of all spills as soon as possible after discovery. Place signs in slippery floor areas to warn occupants of slippery floors. Ensure that operating procedures preclude operating equipment when floor is wet.	III D	3	1	OSHA 1910.22(a)	Open
3.3.03	Failure to clean any spill.	Improper procedures.	Fire/explosion, property damage, personnel injury, death.	IC	Train personnel in proper spill handling actions. Provide necessary equipment and materials.	IE	3	1	OSHA 1910.106;OSHA 1910.120;NFPA 1;Site CHEMICAL HYGIENE PLAN	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Disposal/Waste

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.4.01	Explosive and/or toxic environment developing.	Improper handling or storage of hazardous waste materials inside the facility.	Personnel injury.	IIB	Ensure that all material retained following a spill inside the facility is treated as hazardous waste. Store the waste in approved labeled containers. Take necessary precautions during storage or have the hazardous waste professionally removed from the site.	IID	2	1	OSHA 1910.38;OSHA 1910.120;OSHA 1910.1450;EPA Regulations; Site Chemical Hygiene Plan	Open
3.4.02	Release of toxic, flammable or explosive fumes or liquids.	Failure to provide adequate waste containers in laboratory areas and storage area.	Possible exposure to toxic fumes and fire which may result in personnel injury or death and equipment and facility damage.	IC	Provide suitable disposal containers that are labeled "hazardous waste" and indicate permissible contents. Ensure sufficient quantity of containers are available to allow segregation of solvents, flammables, etc.	IE	3	1	OSHA 1910.106;;Site Chemical Hygiene Plan	Open
3.4.03	Exposure of environment or unprotected personnel to toxic material deposits.	No checking or control of ducts or hoods.	Environmental contamination, unsafe operating areas.	IIB	Ensure that all ducts or hoods, are checked for toxic deposits/build-ups. Dispose toxic deposits appropriately. Develop special procedures for this work.	IIE	3	1		Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Handling/Use

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.5.01	Personnel exposure to various hazardous materials.	Unsafe handling of acids, bases, and solvents, including possible incompatible storage combinations.	Personnel injury or illness.	IIA	Ensure that all appropriate safety measures are undertaken during material handling. Ensure that compatibilities are considered during planning of handling and storage operations.	IIE	3	1	OSHA 1910.1450;;Site Chemical Hygiene Plan	Open
3.5.02	Exposure of hazards to unprotected personnel.	Handling hazardous chemicals and materials in unprotected or unsafe areas (such as office corridors) can expose others to hazards.	Injury to unprotected personnel.	IIB	Ensure that hazardous materials and chemicals are handled only in areas properly designated and protected. Provide separate facility entrances and corridors if required. Provide carts and buckets for transport of chemicals.	IID	2	1	UFC 80;;Site Chemical Hygiene Plan	Open
3.5.03	Fire and/or explosion	Improper operating procedures. Incompatible materials being transferred/ handled/ used react with each other.	Personnel injury and/or equipment damage or loss.	ID	Ensure proper operating procedures. Provide personnel training in safety features. Post signs addressing the use of incompatible materials. Keep incompatible materials separated from each other at all times.	IE	3	2	NFPA 45, NFPA 318;NFPA 49, NFPA 491M	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Material Handling
Subsystem: Bulk Systems

Date: July 11, 1997
Page: 55
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
3.6.01	Loss of liquid nitrogen storage tank integrity.	Premature storage tank corrosion.	Potentially extensive and environmentally harmful ground or groundwater contamination.	IIB	Provide proper material thickness/ type and/or protective coatings for liquid nitrogen storage tank. Consider all applicable standards and recommendations provided in the selection or design of storage tanks.	IID	2	1	NHB 1700.6;ASME Pressure Vessel; and Boiler Code, Sec. VIII	Open
3.6.02	Chemical/process gas leaks from fittings or connections.	Improper design or installation of process gas piping system.	Personnel injury. Impaired vision. Obstruction of passageways.	IIC	Design and install liquid nitrogen process gas piping systems in accordance with industry standards and regulations. Perform quality leak testing.	IIE	3	2	CGA Standards	Open
3.6.03	Loss of storage tank integrity.	Premature storage tank corrosion.	Potentially extensive and environmentally harmful ground or groundwater contamination.	IID	Place storage tanks on re-certification program to ensure storage tank integrity. Provide periodic inspection.	IIE	3	2	NHB 1700.6	Open
3.6.04	Personnel contact w/ liquid nitrogen.	Improper Dewars fill station set-up or faulty containers.	Personnel injury.	IIIC	Provide properly designed fill station and containers.	III E	3	2		Open
3.6.05	Personnel contact w/ liquid nitrogen.	Faulty containers or improper filling procedures at liquid nitrogen dewar filling station.	Personnel injury.	IIIC	Provide proper containers, and procedures for filling containers at liquid nitrogen dewar filling station.	III E	3	2		Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: General Facility
Subsystem: Access/Egress

Date: July 11, 1997
Page: 56
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.1.01	Failure to provide adequate number and arrangement of emergency egress.	Insufficient means of egress. Not enough exits. Poor arrangement of exit locations.	Injury or death to occupants due to improper location or lack of adequate evacuation routes during an emergency.	IIB	Provide adequate number of separate means of egress. Exits shall be located and exit access shall be arranged so that exits are readily accessible at all times.	IIE	3	1	NFPA 101 Sec. 5-4;NFPA 101 Sec. 5-5;OSHA 1910 Subpart E;UBC Ch. 33	Closed
4.1.02	Insufficient capacity of egress.	Every component of means of egress does not provide the minimum required width.	Inability for occupants to leave building in a timely manner. Personnel injury.	IIB	Ensure halls, doorways, and other parts of the exit meet the proper occupant loading in order to provide proper capacity of egress.	IIE	3	1	NFPA 101 Sec. 5-3	Closed
4.1.03	Occupants failure to exit building during fire.	Excessive travel distance to nearest exit.	Injury or death to occupants due to excessive travel distances and spreading fire.	IIB	The maximum travel distance, for this mixed assembly/ business occupancy, shall not exceed 200 ft. to at least one exit.	IIE	3	1	NFPA 101 Sec. 5-6; UBC Ch. 33	Closed
4.1.04	Confused occupants prevented from exiting building.	Excessive dead-end corridors.	Personal injury.	IIB	Dead-end corridors shall exceed 20 feet.	IIE	3	1	NFPA 101 Ch. 26-2.5.2	Open
4.1.05	Occupants failure to reach a public way during a fire.	Failure to provide suitable travel surfaces. The means of egress ends at the point of exit from the building.	Injury to occupants.	IIB	All exits shall terminate at a public way. The public way for ESSB is the road in front of the building. Provide a paved walkway from the exits at the back of the building and office wings to the public way.	IIE	3	1	NFPA 101 Sec. 5-7; NFPA 101 Sec. 31-1.2.2	Closed

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Generagl Facility
Subsystem: Electrical

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.2.01	Increased danger due to failure of critical and/or emergency systems.	Improper design or installation of emergency power systems.	Increased danger of personnel injury/death or property damage.	IB	Design emergency power source & distribution systems in accordance with required regulations and standards.	ID	2	1	OSHA 1910.308(b);NFPA 70, NFPA 110;;UBC 1716(g) & UBC 1807(i) FOR ATRIUM SMOKE-CONTROL SYSTEM.	Open
4.2.02	Continued operation of equipment under dangerous conditions.	Inability to shut off power to equipment in the event of an accident.	Possible death or severe injury to personnel. Equipment damage.	IC	Provide readily accessible power shut-off switches near all equipment and doors to work areas.	IE	3	1	OSHA 1910.305;NFPA 70;NFPA 70E Ch. 3	Closed
4.2.03	Continued operation of equipment under dangerous conditions.	Inability to shut off equipment in the event of an accident.	Possible death or severe injury to personnel. Equipment damage.	IC	Provide readily accessible power shut-off switches on all equipment that do not have hard wired breakers near the equipment. Ensure that all hazardous equipment are provided with appropriate emergency shutdown provisions. Unused pigtails should be	IE	3	1	OSHA 1910.305;NFPA 70;NFPA 70E Ch. 3	Open
4.2.04	Combustion sparks or other ignition sources.	Motors and equipment operating in explosive environment.	Ignition of vapors and/or flammable and combustible liquids, possible explosion, possible injury or death.	IC	All electrical equipment in an explosive environment must be explosion proof. Use spark proof motors in explosive environment.	IE	3	1	OSHA 1910.106;NFPA 30 (Specifically Ch. 4-7.2), NFPA 70;UFC	Closed

Facility Hazard Analysis

Project: Earth Systems Science Building
System: General Facility
Subsystem: Electrical

Date: July 11, 1997
Page: 65
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.3.01	Poor illumination of exits and other means of egress.	Improper design, location, or installation of emergency lighting.	Personnel injury.	IIC	Provide adequate illumination of means of egress. The floors within an exit and within the portions of the exit access and exit discharge (inside the building) shall be illuminated to values of not less than 1 footcandle measured at the floor.	IIE	3	2	NFPA 101 Sec. 5-8;UBC Sec. 3313;UFC Sec. 12.110	Closed
4.3.02	Occupants cannot find their way to an exit.	No lighting for emergency egress following a power outage in the facility.	Personnel injury.	IIC	Provide emergency lighting systems for the means of egress. Where illumination depends on changing energy sources, there shall be no appreciable interruption of illumination. Emergency illumination shall be provide for 1 1/2 hours in the event of	IIE	3	2	NFPA 101 Sec. 5-9;UBC Sec. 3313;UFC Sec. 12.110	Open
4.3.03	Failure of occupants to reach a public way during a fire.	The discharge from exit does not have adequate lighting to the public way.	Injury to personnel.	IIB	The concrete walkway leading from the exits at the back of the building and office wings to the public way should be illuminated and marked to make clear the direction of egress to the public way.	IIE	3	1	NFPA 101 Sec. 5-7;NFPA 101 Sec. 5-8	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: General Facility
Subsystem: Structural

Date: July 11, 1997
Page: 67
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.4.01	Laboratory floor collapse.	Inadequate floor load design.	Personnel injury and/or death or equipment damage or loss due to floor collapse.	IC	Consider all possible objects, weights of equipment, stored inventory and personnel when designing for floor loads.	IE	3	1	NHB 7320.1B Ch. 6;UBC;OSHA 1910.12;OSHA 1910.22	Closed
4.4.02	Floor collapse (other than laboratory).	Inadequate floor load design.	Personnel injury and/or death or equipment damage or loss due to floor collapse.	IC	Consider all possible objects, weights of equipment, stored inventory and personnel when designing for floor loads.	IE	3	1	NHB 7320.1B Ch. 6;UBC;OSHA 1910.12;OSHA 1910.22	Closed
4.4.03	Roof collapse.	Inadequate loading requirements used in structural design.	Personnel injury or death. Equipment or property damage and/or loss.	IC	Consider all types of anticipated loading when designing roof structures. Consider roof operations and mechanical/electrical equipment on roof.	IE	3	1	NHB 7320.1B Ch. 6;OSHA 1910.12;OSHA 1910.22	Open
4.4.04	Wall collapse.	Inadequate loading requirements used in structural design.	Personnel injury or death. Equipment or property damage and/or loss.	IC	Consider all types of anticipated loading when designing walls. Include design of heavily loaded wall cabinets.	IE	3	1	NHB 7320.1B Ch. 6	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: General Facility
Subsystem: Elevators

Date: July 11, 1997
Page: 69
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.5.01	Failure of elevator system.	Elevator system not designed to meet loads of required usage.	Personnel injury and/or equipment damage or loss.	IID	Ensure proper design of elevators. Design of passenger elevators should include regular work in addition to conference and cafeteria traffic from people not normally using the facility. Freight elevator should include loads from heavy equipment (lab	IIE	3	2	ASME/ANSI Sec. A17.1-A17.3	Open
4.5.02	Failure of elevator system.	Improper operating procedures (exceeding weight limits). Accidental release of safety latch.	Personnel injury and/or equipment damage or loss.	IID	Ensure proper elevator operating procedures. Provide personnel training in safety features and load limits. Ensure heavy equipment is moved only in the freight elevator. Post signs regarding weight limits.	IIE	3	2	ASME/ANSI Sec. A17.1-A17.3	Open
4.5.03	Failure of electric lifts or other failure in elevators.	Lack of proper, preventive maintenance program.	Personnel injury and/or equipment damage or loss.	IIC	Establish effective preventive maintenance for elevators.	IE	3	2	ASME/ANSI Sec. A17.1-A17.3	Open
4.5.04	Failure of elevator system.	Hoist fails or faulty electrical design/work.	Personnel injury and/or equipment damage or loss.	IID	Provide safety measures for runaway car, and for electrical work (grounding, etc.)	IIE	3	2	NFPA 70 Article 620	Open
4.5.05	Fire spreading to elevator.	Elevator shaft is not separated from the remainder of the building by a fire-rated enclosure.	Personnel injury or major property damage.	IC	Contain fire by providing a two-hour fire rated elevator assembly/ shaft. Elevator car doors shall have a 1 1/2 hour fire rating.	IE	3	1	UBC 5102, UBC 1706;ASME/ANSI A17.1;NFPA 80 Ch. 8	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: General Facilities
Subsystem: General

Date: July 11, 1997
Page: 71
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
4.6.01	Lightning.	Natural phenomena. Inadequate grounding of lightning protection system.	Electrocution resulting in injury or death. Fire resulting from lighting strike.	IC	Provide adequate grounding of lightning protection system.	IE	3	1	NFPA 780;NFPA 70	Closed
4.6.02	Inadvertent release of high pressure steam.	Poor design or workmanship of steam system components, or poor operation.	Possible injury or system failure.	IIIC	Review system design to ensure it meets code and standard requirements. Develop safe operating procedures for steam system in accordance with applicable codes and standards.	IIIE	3	2	UMC Ch. 21	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Documentation
Subsystem: Emergency Preparedness

Date: July 11, 1997
Page: 72
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
5.1.01	Continued flow of utilities (electrical power, gases, water, etc.) Under unsafe conditions or in emergency situation.	Inability to deactivate utilities in the event of an accident. Lack of emergency shut-off switches.	Possible severe injury or death to personnel. Property damage or loss.	IB	Ensure all utilities have easily accessible and well labeled emergency shut-off switches. Provide access to electrical vault.	IE	3	1	NFPA 70 Article 230-70;NFPA 70 Article 230 Part F;NFPA 70 Article 670-4	Open
5.1.02	Continued operation of safety critical equipment or flow of utilities to equipment under unsafe conditions or in emergency situation.	Inability to deactivate equipment and/or utilities to equipment in the event of an accident. Lack of emergency shut-off switches	Possible severe injury or death to personnel. Property damage or loss.	IB	Ensure all sources of energy (equipment power sources and utilities to equipment) have easily accessible and well labeled emergency shut-off switches, valves, etc.	IE	3	1	NFPA 70 Article 230-70;NFPA 70 Article 230 Part F;NFPA 70 Article 670-4	Open
5.1.03	Continued and/or discontinued operation of equipment connected to the motor control centers (mcc), and emergency motor control centers (emcc)	Inability to quickly assess an emergency situation. Possibility of activating and/or de-activating the wrong piece of equipment.	May cause severe injury to persons unaware of situation.	IID	Provide labels to describe the motor control centers, and emergency motor control centers (emcc) panels in detail. For example describe (number) an exhaust fan, its location, and any hazardous materials emitted from it. Provide extra fuses for emccs.	IIE	3	2		Open
5.1.04	Inadequate knowledge of fire procedures.	Failure to conduct fire drills on a regular basis.	Increased danger of personnel injury or death.	IC	Conduct fire exit drills regularly with coordination from local authorities.	IE	3	1	NHB 1700.1(V1-B) Ch. 4;NFPA 101 Ch. 31-1.5;NSS 1740.11 Par. 604(d);NSS 1740.11 Par. 803	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Documentation
Subsystem: Test Procedures

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
5.2.01	Out-of-spec and unsafe equipment. Unsafe operation of relocated, used equipment.	Moving existing machinery to new location could effect its operation or safety, due to damage during moving, new set-up, etc.	Personnel injury or death and property damage or loss due to accidents resulting from operation of unsafe equipment.	IA	Properly test & certify all relocated equipment to meet operating specifications after being moved to new location and prior to starting normal operations.	ID	2	1	OSHA 1910.212	Open
5.2.02	Damage to equipment caused by poor equipment design or improper installation.	Inadequate testing to assure proper equipment operation prior to use.	Malfunctioning or failed equipment causing personnel injury.	IIB	Conduct pre-operation/ acceptance tests of all equipment installed during construction phase.	IIE	3	1	NFPA 70, NFPA 70E	Open
5.2.03	Damage to equipment caused by poor equipment design or improper installation during laboratory installation phase.	Inadequate testing to assure proper equipment operation prior to use.	Malfunctioning or failed equipment causing personnel injury.	IIB	Conduct pre-operation/ acceptance tests of all equipment installed during lab installation phase.	IIE	3	1	NFPA 70, NFPA 70E	Open
5.2.04	Dangerous operating conditions caused by concurrent construction and testing.	Testing required to continue during construction project.	Possible personnel injury, death, or system damage or loss.	IA	Avoid unnecessary testing during construction, and establish adequate controls and procedures to minimize danger if testing must be conducted concurrent with construction.	IE	3	1	USER CONFIGURATION CONTROL PLAN	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Documentation
Subsystem: Operational Procedures

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
5.3.01	Unsafe and unauthorized operating procedures.	Lack of proper documentation for approved operating procedures, leading to unsafe practices during operations.	Personnel injury or equipment damage.	IIC	Provide comprehensive operations manual to incorporate all operational, material handling, repair, and maintenance procedures. Should include system operation, interfaces, and appropriate hazards associated with each operation.	IIE	3	2	User Configuration Control Plan; User Operation and Maintenance (O&M) Manuals	Open
5.3.02	Unsafe operations during operational phases.	Lack of or inadequate control measures established and followed during equipment installation and operation.	Personnel injury, equipment damage.	IIB	Ensure that management establishes control measures to minimize unsafe or uncontrolled operations.	IIE	3	1	User Configuration Control Plan	Open
5.3.03	Chemical burns, eye damage, contaminated personnel and fire or explosion.	Failure to develop standard analytical procedures and determine potential hazards regarding procedures. Failure to provide safety training for analytical procedures.	Personnel injury. Possible skin disorders. Increased risk of equipment loss and facility damage due to fire.	IIB	Develop standard analytical procedures for lab use. Perform a hazards analysis of procedures. Train personnel on analytical procedures.	IID	2	1	NSC - Fundamentals Of Industrial Hygiene	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Documentation
Subsystem: Maintenance Procedures

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
5.4.01	Inadequate protection offered by personal protective equipment.	Unchecked deterioration due to inadequate inspection and maintenance.	Personnel injury and/or death due to exposure to hazardous materials or fire. Equipment and facility damage or loss due to fire.	IB	Establish comprehensive preventative maintenance, testing and inspection program for personal protective equipment. Test and certify all respirators, masks, filters, etc.	IE	3	1	OSHA 1910 Subpart I; OSHA 1910.34; Site Chemical Hygiene Plan	Open
5.4.02	Damage to equipment or system failure / degradation.	Inadequate / improper preventative maintenance procedures.	System and equipment damage, possible personnel injury.	IB	Provide recommended (as appropriate or by manufacturer) checks of critical equipment to ensure safe operational conditions. Institute a preventative maintenance program to keep up effectiveness and safety of system and equipment.	IE	3	1	NFPA 70, NFPA 70E; USER OPERATION And MAINTENANCE (O&M) Manuals; User Configuration Control Plan	Open
5.4.03	Possible explosion or ignition of fumes in work area during maintenance procedures.	Unsafe maintenance procedures.	Injury or death of personnel from lack of safety considerations during maintenance procedures.	IB	Do not begin any maintenance work until all explosive or flammable vapors have been removed from area. All metal objects should be grounded, and only spark resistant tools should be used.	IE	3	1	OSHA 1910.106;NFPA 30, NFPA 91;GMI 1700.4 "Hot Work Permit"	Open
5.4.04	Stationary/ fixed chemical tank/ cylinder explosion and fire.	Lack of and/or improper tank/ cylinder maintenance and inspection procedures.	Personnel injury or death. Property damage or loss. Personnel asphyxiation.	ID	Provide for safe and appropriate stationary/ fixed chemical tank/ cylinder maintenance. Insure personnel are properly equipped.	IE	3	2	NFPA 45;NHB 1700.6	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Documentation
Subsystem: Training

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
5.5.01	Release of toxic, flammable or explosive fumes or liquids inside the facility or to the environment with increased risk of fire, explosion or exposure to toxic materials.	Failure to provide adequate training for identification, collection, packaging and storage of hazardous wastes.	Environmental contamination may result. Possible personnel injury or death may occur. Equipment, personal property or facility damage may also occur.	IB	Provide training on procedures for identification, collection, packaging, storage, and response to hazardous materials incidents.	IE	3	1	OSHA 1910.106;NFPA 30;;Site Chemical Hygiene Plan	Open
5.5.02	Excessive exposure to toxic and hazardous materials.	Inadequate training.	Fire resulting in personnel injury and/or death and equipment and facility damage or loss. Personnel exposure to toxic chemicals resulting in personnel injury and/or death. Environmental damage due to release of hazardous materials.	IB	Provide regular, comprehensive training for laboratory personnel. Training should meet the minimum requirements of the indicated references.	IE	3	1	OSHA 1910.134;OSHA 1910.1200;OSHA 1910.1450;;Site Chemical Hygiene Plan	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Facility Operation
Subsystem: Laboratory Design

Date: July 11, 1997
Page: 85
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
6.1.01	Spread of fire within laboratory hoods.	Improper or combustible (such as polypropylene) materials used for hood construction. Significant increase in combustible loading.	Contribute to rapid spread of fire resulting in personnel injury, death, and equipment and facility damage.	IB	Laboratory hoods should be constructed of materials having a flame spread index of 25 or less, and an acceptable smoke spread rating when tested in accordance with NFPA 255.	IE	3	1	NFPA 45 Ch. 6-9;NFPA 255	Open
6.1.02	Propagation of fire in hoods, or other areas not covered by general sprinkler system.	Inadequate fire protection, such as non-sprinkler protected hoods in areas where build-ups of flammable or explosive fumes occur, or in hoods made of combustible material.	Personnel injury or death, equipment or facility damage or loss.	IB	Install sprinklers in fume hoods where flammable or explosive fumes could migrate or accumulate, and in hoods made of combustible material.	IE	3	1	NFPA 45 Ch. 6	Closed
6.1.03	Propagation of fire in gas cabinets or other vented enclosures (areas not covered by general sprinkler system).	Toxic or highly toxic gases leaking from cylinder. Fire gas storage cabinet.	Personnel injury or death, equipment or facility damage or loss.	IB	Gas cabinets or exhausted enclosures for the storage or use of toxic or highly toxic gas cylinders shall be internally sprinkler protected.	IE	3	1	UFC 80.303(a)(3)(B);UFC 80.402(b)(2)(D)	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Facility Operations
Subsystem: Computer Rooms

Date: July 11, 1997
Page: 89
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
6.2.01	Fire in tape storage area. Fire spreading to tape storage area.	Record (tape storage) not separated from the remainder of the facility by 2-hour fire-resistive construction.	Toxic fumes developing from burning plastics. Essential data on tapes is lost.	IC	Separate the record storage areas from the remainder of the facility by 2-hour fire-resistive construction per nss 1740.11.	IE	3	1	NSS 1740.11 Ch. 703(f);NFPA 75 Sec. 7-2	Open
6.2.02	Fire spreading to computer rooms.	Lack of fire resistive occupancy separation.	Major computer and data loss.	IIB	The computer area shall be separated from other occupancies within the building by fire-resistant rated construction of not less than one-hour.	IIE	3	1	NFPA 75 Sec. 3-1.3;NSS 1740.11 Par. 703(f)	Closed
6.2.03	Fire spreading to computer rooms.	Lack of fire resistive occupancy separation.	Major computer and data loss.	IIB	The computer room shall be separated from other occupancies in the computer area by fire-resistant rated construction of not less than one-hour.	IIE	3	1	NFPA 75 Sec. 3-1.3;UBC Table 17-A	Open
6.2.04	Fire spreading to computer rooms.	Poor location of computer rooms in building.	Major computer and data loss.	IIB	Steam, water, or horizontal drain piping should not be in the space above the suspended ceiling and over computer equipment other than for sprinkler system use. Basement areas should not be considered for the location of a computer area. If computers	IIE	3	1	NFPA 75 Sec. 3-2.1;NFPA 75 Sec. 3-3.2	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Facility Operations
Subsystem: Lasers

Date: July 11, 1997

Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
6.3.01	High energy release, shocks.	Ungrounded laser power supply.	Fire, injury, death.	IB	Provide fuses, circuit breakers, insulation, grounding, interlocks, etc., As necessary to prevent shocks and accidental high energy releases from laser power supplies.	ID	2	1	ANSI Z136.1;NSC Fund. of Indust. Hyg., Chapter 11	Open
6.3.02	High energy release.	Unprotected capacitors (laser power supply).	Fire, injury, death.	IB	Isolate laser power supply capacitors with screens, shields, barriers, or uninhabited rooms. Doors and covers shall be interlocked.	IE	3	1	ANSI Z136.1, Sec. 4.6.3, 4.6.4	Closed
6.3.03	Accumulated combustibles in hazardous areas.	Poor housekeeping.	Fire.	IIC	Maintain the laser target areas clean and clear of combustibles or flammable liquids.	IIE	3	2	ANSI Z136.1	Open
6.3.04	Accumulation of hazardous by-products from lasers.	Poor housekeeping, inadequate control of hazardous materials.	Fire, injury.	IIC	Provide proper containment and disposal of hazardous by-products from laser operations.	IIE	3	2	ANSI Z136.1, Sec. 7.3	Open
6.3.05	Unauthorized personnel in laser operation area.	No warning devices.	Personnel injury.	IIC	Provide necessary warning signs and devices to alert personnel of hazardous laser operations.	IIE	3	2	ANSI Z136.1, Sec. 4.3.9, 4.3.15, 4.7	Closed
6.3.06	Exposure of eyes to laser beam.	Improper laser position.	Personnel eye injury.	IIC	Laser beam elevation should be maintained at a level other than the normal position of the eyes of personnel in the standing or seated position.	IIE	3	2	ANSI Z136.1, Sec. 4.1	Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Facility Operations
Subsystem: Clean Rooms

Date: July 11, 1997
Page: 96
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
6.4.01	Recirculation of hazardous or flammable fumes from spill or leak in cleanroom.	Cleanroom design of air circulation system allows recirculation of air from areas with possible fume accumulations.	Personnel sickness or injury.	IIA	Ensure that cleanroom air cannot be recirculated in any areas where hazardous or flammable materials/ gases may be spilled. Provide maximum practical fresh air. Minimize dead air spaces.	IID	2	1		Open
6.4.02	Chemicals migrating to other parts of building during emergency in cleanrooms.	Chemical spill and/or equipment failure.	Personnel injury.	IIC	During emergencies cleanroom air shall have negative pressure relative to outside air, so no air (containing flammable/toxic fumes) will flow out of the cleanrooms.	IIE	3	2		Open

Facility Hazard Analysis

Project: Earth Systems Science Building
System: Facility Operations
Subsystem: General

Date: July 11, 1997
Page: 97
Prepared by: Wal Syphrum

Control Number	Hazard Description	Causes	Effects	SP-1	Recommendations	SP-2	HRI 1	HRI 2	References	Status
6.5.01	Fire spreading.	Combustible materials and/or chemicals storage.	Catastrophic injury, possible system loss.	IC	Keep all building areas (including utility tunnel) free of combustible materials and chemicals to minimize risk of fire spreading.	IE	3	1	Site CHEMICAL HYGIENE PLAN;UBC Sec. 3305(a);UFC;NFPA 101 Sec. 5-5.1.7	Open
6.5.02	Increased danger of personnel. Injury/ death and property damage/ loss due to lack of communication, lack of inter facility coordination, and lack of centralized control and monitoring.	System/subsystem interfaces and facility enclosure interdependencies not considered in the planning and design of building.	Increased danger of personnel injury, death, and property damage or loss due to fire or other hazardous situation.	IB	Consider the interdependencies and interfaces of all facility systems (i.e. ventilation, electrical, fire protection, etc.) In relation to enclosure and the design of the support & services building.	ID	2	1		Open