Document Number:	GLM-QS-1700.1.3
Revision:	Basic
Effective Date:	**10/18/2010**
Expiration Date:	10/18/2017

Glenn Safety Manual – Chapter 3

Facility System Safety w/Change 4(5/24/2016)

Approved by: QS/Chief, Safety and Health Division

Distribution: BMS Library

NASA - Glenn Research Center
Cleveland, OH 44135

Change Record

Rev.	Effective Date	Expiration Date	GRC25, Change Request #	Description
Basic	10/18/2010	10/18/2015	Basic	
Change 1	4/14/2014	10/18/2015	N/A	Administrative changes to add front cover and change history log to comply with NPR 1400.1 and added "The GRC shall follow the requirements of" in Section 6.0 Requirements
Change 2	9/30/2015	10/18/2015	N/A	Administrative change to remove hyperlinks.
Change 3	1/5/2016	10/18/2016	N/A	Administrative change to extend the expiration date to October 18, 2016, due to anticipated changes in Agency policy.
Change 4	5/24/2016	10/18/2017	N/A	Administrative change to extend the expiration date to October 18, 2017, due to anticipated changes will allow orderly and effective transition to new policy requirements without lapse in overall safety policy.

***Include all information for each revision. Do not remove old revision data. Add new rows to table when space runs out by pressing the tab key in the last row, far right column.*

Contents

1.0 PURPOSE 4
2.0 APPLICABILITY 4
3.0 BACKGROUND 4
4.0 POLICY 5
5.0 RESPONSIBILITIES 5
5.1 Plum Brook Management Office (PBMO), Facility Project Manager, or Designated Facility Manager/Coordinator 5
5.2 Chief, Facilities Division and Plum Brook Management Office (PBMO) 5
5.2.1 System Managers 6
5.2.2 Configuration Manager 6
5.2.3 Project Manager 6
5.3 Facility Hazard Analysis (FHA) Preparers 6
5.4 Chief, Safety and Health Division (SHeD) 7
5.4.1 Facility System Safety Program Lead 7
5.5 Facility System Safety Committee 7
5.6 Safety, Health and Environmental Board and Operations Management Council 8
6.0 REQUIREMENTS 8
6.1 Facility Safety Management Plan 8
6.1.1 Facility Risk Indicator (FRI) 9
6.1.2 Preliminary Hazard List (PHL) 9
6.1.3 Facility Hazard Analysis (FHA) 10
6.1.4 Hazard Analysis Tracking Index (HATI) 10
6.1.5 Facility Configuration Management Process 10
6.2 New Facilities and Systems 10
6.3 Existing Facilities and Systems 11
6.4 Facility Hazard Analysis Preparation 11
6.4.1 Facility Hazard Analysis Organization 11
6.4.2 Facility Hazard Analysis Phases of Preparation 12
6.4.3 Hazard Analysis (HA) 13
6.4.4 Risk Assessment 13
6.5 Glenn Research Center Interlock Philosophy 15
6.5.1 Design 15
6.5.2 Engineered Safety Features 15
6.5.3 Safety Devices 15
6.5.4 Warning Devices 15
6.6 Training 16
7.0 RECORDS 16
8.0 REFERENCES 16
APPENDIX A.—DEFINITIONS AND ACRONYMS 17
APPENDIX B.—FACILITY RISK INDICATOR (FRI) EVALUATION 19
APPENDIX C.—FACILITY SAFETY MANAGEMENT PLAN (FSMP) OUTLINE 23

List of Tables

TABLE 6.1.—SEVERITY CATEGORIES 13
TABLE 6.2.—PROBABILITY OF OCCURRENCE GUIDELINES 14
TABLE 6.3.—RISK LEVEL MATRIX 14

List of Figures

Figure 6.1.—GRC Facility System Safety Program activities 11

Chapter 3—Facility System Safety

NOTE: *The current version of this chapter is maintained and approved by the Safety and Health Division (SHeD). This chapter was created in September 2010. The current version is located on the Glenn Research Center intranet within the BMS Library. Approved by Chief of Safety and Health Division.*

1.0 PURPOSE

This chapter sets forth the requirements in the Facility System Safety Program for the Glenn Research Center (GRC) at both Lewis Field and the Plum Brook Station. It describes the responsibilities pertaining to facility system safety of supervisors, and employees, including Safety and Health Division (SHeD) personnel.

The GRC Facility System Safety Program exists to ensure the safe and continuous operation of GRC facilities. It is intended to ensure that the appropriate level of safety analysis, oversight, and resources are applied to projects involved in the construction of facilities (CoF) process as well as modifications made to existing facilities.

The GRC Area Safety Committee Safety Permit Process (Glenn Safety Manual, Chapter 1A) covers the operation of research test systems and central process systems.

2.0 APPLICABILITY

The provisions of this chapter are applicable to all NASA employees and to all other agencies, organizations, and contractor personnel who are involved in facility acquisition, modification, test activities, operations, maintenance, and disposal of facilities at GRC Lewis Field or Plum Brook Station. It is applicable to CoF projects and all facility life-cycle phases.

3.0 BACKGROUND

The GRC Facility System Safety Program includes two major components: safety analysis, which can be in the form of a facility hazard analysis (FHA), standard operating procedure (SOP), safety permit, or other means of documented analysis, and facility configuration management (CM) process, which is detailed in GLP–FB–8820.1, Configuration Control of Facilities.

System safety engineering is an approach used to identify deficiencies in system or facility design and acquisition, modification, associated testing, and operational sequences that 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 engineering within the facility acquisition process. The objectives of a facility system safety program are

- To ensure that hazards inherent to the design and equipment intended for use in 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 to facility designs
- To ensure that modifications do not increase the risk level of a

facility The GRC Facility System Safety Program intends to

- Ensure that the appropriate safety analysis has been conducted; the objectives are to
    - Define the hazards in terms of severity and probability
    - Assess the controls for those hazards
    - Make recommendations toward reduction of the severity and/or probability of occurrence

- Ensure that designated facilities and systems have the appropriate level of allocated safety resources
- Document risk and provide the information to management and operating personnel

The Facility CM Program establishes a baseline and maintains current records for designated systems (e.g., electrical systems) and the relevant documentation (e.g., drawings), showing changes and modifications through the life cycle of the facility. The program allows for proper review of proposed changes.

4.0 POLICY

It is GRC policy that facilities and systems at Lewis Field and the Plum Brook Station shall be designed, operated, and maintained to adequately control hazards likely to cause physical harm to personnel or severe system damage.

The authority for this program is outlined in NASA Procedural Requirement (NPR) 8715.3C, NASA General Safety Program Requirements, and supported by NASA Standard (STD) 8719.7, Facility System Safety Guidebook, and NPR 8820.2, Facility Project Requirements. These standards and requirement documents outline specific processes and tasks that are to be carried out for the acquisition and operation of facilities (see Section 6.0, Requirements).

5.0 RESPONSIBILITIES

Facility system safety is only accomplished through a team effort of individual organizations accepting their roles in the overall objective to maintain the appropriate level of safety analysis, oversight, and resources to projects involved in the CoF process as well as modifications made to existing facilities. Specific responsibilities of individuals or organizations tasked with requirements to support the Facility System Safety Program follow.'

5.1 Plum Brook Management Office (PBMO) Facility Project Manager, or Designated Facility Manager/Coordinator

- Identify projects and facility or system changes that must adhere to the Facility System Safety Program and provide the resources necessary to implement the program
- Assist in the determination of the facility risk indicator (FRI) (see Section 6.6.1)
- Initiate the Facility Safety Management Plan (FSMP)
- Oversee the development and/or review of an FHA (see Section 6.1.3)
- Verify the hazard controls documented in the FHAs are part of the design and/or operations of the facility
- Oversee the review of applicable updates to the FHAs and revise should any changes occur in the hazards or hazard controls; report risks that meet appropriate criteria to management
- Seek assistance from SHeD, as needed, in completing and reviewing FHAs
- Ensure compliance with GRC configuration control requirements (The facility shall not be considered complete and ready for operation without all equipment files and/or facility and system drawings (as-built) being provided to the Configuration Manager for permanent file and drawing updates.)
- Upon completion of the facility construction or modification, assume ownership of the FSMP
- Maintain system safety training records for applicable personnel
- Serve as a member of the Facility System Safety Committee when required to review FRI or FSMPs associated with the Facility Manager's facility

5.2 Chief, Facilities Division and Plum Brook Management Office (PBMO)

- Oversee and manage functions associated with system management, CM, and project management
- Participate in the Facility System Safety Committee to analyze and approve the FSMP, as required, to manage level-1 and level-2

5.2.1 System Managers

- Identify facility system changes that must adhere to the Facility System Safety Program and ensure that the required resources necessary to implement the program are in place
- Ensure identified facilities can be constructed or modified without jeopardizing system requirements or capabilities
- Ensure that any new or unforeseen risks that may arise during the construction or modification of a facility are immediately brought to the attention of the Facility Manager
- Ensure that proper configuration control and management are followed and that all equipment files and/or facility and system drawings are properly updated (The task cannot be closed nor can the facility be considered complete without this occurring.)
- Participate as a member of the Facility System Safety Committee, when required

5.2.2 Configuration Manager

- Manage the identification of projects and facility or system changes that must adhere to the Facility System Safety Program
- Manage the records associated with establishing, maintaining, and utilizing designs, schematics, plans, and graphics associated with GRC facilities and systems
- Maintain the FRI and FMSP as records in the GRC CM process and databases
- Alert the Facility Manager when any new or unforeseen risks that may arise during the construction or modification of a facility
- Ensure that proper configuration control and management are followed and that all equipment files and/or facility and system drawings are properly updated
- Participate as a member of the Facility System Safety Committee

5.2.3 Project Manager

- Identify projects and facility or system changes that must adhere to the Facility System Safety Program and ensure that the required resources necessary to implement the program are in place
- Ensure identified facilities can be constructed or modified without jeopardizing system requirements or capabilities
- Alert the Facility Manager when any new or unforeseen risks that may arise during the construction or modification of a facility
- Ensure that proper configuration control and management are followed and that all equipment files and/or facility and system drawings are properly updated (The task cannot be closed and the facility considered complete without this occurring.)
- Participate as a member of the Facility System Safety Committee, when required

5.3 Facility Hazard Analysis (FHA) Preparers

- Develop and maintain a preliminary hazard list (PHL)
- Participate in the development and maintenance of an FHA
- If SHeD is not the primary preparer or facilitator, seek assistance from the SHeD, as needed, in completing FHAs and provide completed FHAs to SHeD for review
- Present PHL and FHA to the Facility System Safety Committee when an FSMP may be required

5.4 Chief, Safety and Health Division (SHeD)

- Establish and maintain adequate policies and procedures for the application of the Facility System Safety Program

- Assign a Facility System Safety Program lead to
    - Assist GRC organizations with FHA development and establishment of necessary team membership and other resources
    - Facilitate FHAs, when required
    - Review FHAs
    - Review and assist the effort to establish the FRI
    - Audit the hazard analysis tracking index (HATI) during a project to ensure that hazard controls outlined in the FHA are included during construction
    - Report risks that meet appropriate criteria to management
    - Provide support to the Facility and Project Managers to ensure the FSMP is up to date
- Participate as a member of the Facility System Safety Committee
- Assign members, including the Chairperson, to the Facility System Safety Committee

5.4.1 Facility System Safety Program Lead

- Provide consultation concerning policies and procedures for the application of the Facility System Safety Program
- Assist GRC organizations with FHA development and establishment of necessary team membership and other resource
- Facilitate FHAs, when required
- Review FHAs
- Review and assist the effort to establish the FRI
- Audit the HATI during a project to ensure that hazard controls outlined in the FHA are included during construction
- Report risks that meet appropriate criteria to management
- Provide support to the Facility and Project Managers to ensure the FSMP is up to date
- Participate as the facilitator and recorder for the Facility System Safety Committee

5.5 Facility System Safety Committee

The purpose of the Facility Safety Committee is to discuss, review, and approve or decline the FSMP for any facility requiring an FSMP per NASA STD 8719.7, Facility System Safety Guidebook, and this GRC Safety Manual chapter.

Primary Membership is composed of Chief, SHeD; Chief, Facilities Division; Director, Plum Brook Station; and Chief, Testing Division or their designated representatives. Supporting members include Facility Configuration Manager and Facility System Safety Program lead. As-needed members include any Facility Manager, Systems Manager, or Project Manager whose facility or project is being reviewed. The meeting schedule is determined by the Chairperson. The committee's responsibilities include

- Issuing Facility System Safety Committee concurrence for an approved FSMP
- Ensuring FSMP is recorded as part of the specific facility configuration database or records storage process
- Soliciting knowledgeable temporary members needed to evaluate the FSMP associated with specific facilities

5.6 Safety, Health and Environmental Board and Operations Management Council

The Safety, Health and Environmental Board (SHEB) and Operations Management Council (OMC) are responsible for making decisions and setting priorities on risks reported by the project or facility.

6.0 REQUIREMENTS

The GRC shall follow the requirements of NPR 8715.3, Chapter 8; and NPR 8719.7.

6.1 Facility Safety Management Plan (NPR 8715.3, Chapter 8; and NASA STD 8719.7, Chapter 5)

Chapter 8 of NPR 8715.3C requires that specific safety tasks to be accomplished during construction, operation, maintenance, and final disposition of a facility are documented in an FSMP in accordance with NPR 8820.2, Facility Project Implementation Guide, and NASA STD 8719.7, Facilities System Safety Guidebook.

NASA STD 8719.7, paragraph 5.2.5.2, requires that an FSMP be created for certain higher risk facilities. These are defined by an FRI of 1 or 2 as discussed below.

The FSMP documents recommended safety efforts for the life cycle of the facility including methods of hazard identification and the resolution process.

The FSMP shall 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 HATI) 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, installation, or testing, do not impact safety
- Facility and system drawings and key operating documents are maintained to properly represent the current condition
- 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
- Facility safety disposal is established with clear procedures and methods

A major portion of the FSMP is identification of hazards and risk through use of an FHA. The FHA is a multistep, team-oriented approach to hazard and risk assessment that begins at the earliest phase of a project and continues throughout the life of the systems involved. Configuration control, or management of change, is also a major portion of the FSMP or any facility system safety program. It is the process that ensures that changes made during the design or construction of new facilities, or proposed changes to existing facilities, are properly reviewed.

The FSMP will include the FRI, the PHL, all FHAs, the HATI, and the configuration control process. These elements are discussed below to provide guidance. Depending on the life-cycle phase of the facility or project and the nature of the systems, other materials and references needed to meet the above requirements of the FSMP should also be included. These may include a reference to required or existing operational safety permits, certification requirements of systems (i.e., pressure system certification), training requirements, chemical management plans, scheduled maintenance of critical equipment, or facility inspections.
The FSMP and the configuration management process will include a method to evaluate all changes to a facility and to determine the proper review path. For example, changes identified as “administrative” or “replacement in kind” normally will not need further system safety review. Changes affecting the configuration of a system will require a system safety engineering analysis. The degree of analysis will depend on the extent and nature of the change and may include a review of SOPs, checklists, engineering drawings, emergency procedures, and training requirements. The FSMP will identify the method of these evaluations and reviews depending on the type of facility or project status such as new facility or system design and construction (generally CoF), existing facility change requests (FCRs), or operating or test system (safety permit process). A sample FSMP outline is given in Appendix B.

6.1.1 Facility Risk Indicator (FRI) (*NPR 8715.3*)

The first step in the system safety process is the determination of the FRI. The FRI classifies the severity of potential hazards inherent to the facility itself: its operations, processes, environment, equipment, potential interfaces, and personnel. 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 FRI is based on the hazards present alone and not the existing or expected mitigation. The mitigation or safeguards are considered in subsequent hazard analysis to assess adequacy of design and safety systems and establish operational risks. The FRI establishes the potential severity and need for a system safety plan over the life cycle of the facility or system. The FSMP is put in place to ensure proper safeguards are maintained for hazards present over the lifetime of the facility.

It is this initial safety assessment that is used to help determine the level of system safety effort required to meet NASA safety requirements. It alerts the Facility or Project Manager and other acquisition managers of the potential safety concerns within a facility. For a new facility, the FRI will be done early in the project life cycle during the project planning and development phase. The determination of a FRI will be performed in accordance with NASA STD 8719.7, Facility System Safety Guidebook (definitions of FRI 1 to 4 are given), and is a cooperative effort between SHeD and facility and project personnel. A checklist such as one given in Appendix C may be used to assist in the determination. The potential hazards inherent to the facility are evaluated using the following criteria as evaluation factors:

- Life safety.—hazards that 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 that could cause serious damage to facilities or equipment resulting in significant financial loss
- Environmental impact.—hazards that could have serious impact to the adjacent facilities or operations or to the surrounding community

A narrative explaining the result should be provided and maintained in the FSMP and or facility documentation.

6.1.2 Preliminary Hazard List (PHL) (*NPR 8715.3*)

Concurrent with FRI establishment is the process to develop the PHL. The PHL identifies and lists 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 for the facility system safety effort and provides input for the FHA. There are various methods used to develop PHL. They include

- 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
- Reviewing the project management plan

Preparing the PHL must encourage the free flow of ideas among those participating. During the development of the PHL, no hazard identified is to be “thrown out.” Credibility of the hazard will be determined during the analysis process, and noncredible hazards will be eliminated at that time.

6.1.3 Facility Hazard Analysis (FHA) (NPR 8715.3)

The FHA is an expansion of the FRI and PHL and is performed and continually revised in the planning and design phases of a project. The assessment of the facility's hazards permits refining and expanding the risk classification of the FRI. It expands upon the PHL and provides the following additional information:

- Details concerning necessary and planned corrective action
- Increased detail of hazards already identified
- More detailed analysis to identify additional hazards

The FHA is used to determine the system safety effort for the remainder of the project. As an expanded version of the PHL, the FHA contains greater detail in three areas. First, hazard control information is added to the identified hazards. Second, a more comprehensive and systematic analysis to identify additional hazards is performed. Third, greater detail on hazards previously identified in the PHL is provided. Detailed knowledge of all operations to be conducted within the facility and any hazards presented by nearby operations is required. Based on the best available data, including lessons learned, hazards associated with the proposed facility design or functions are evaluated for risk severity and probability, together with operational constraints.

If the FHA (see Section 6.4 for preparation) indicates that the facility represents an acceptable level of risk and no further analysis is necessary (see Section 6.4.3), a list of applicable safety standards and codes are still required. If the facility represents an unacceptable level of risk, methods to control risk must be instituted and the status reported to the SHEB and OMC. The FHA is used to establish an HATI, using the analysis tables, and to identify additional analyses, if necessary. Existing hazard analyses may be used in lieu of developing a new FHA. FHAs are configuration controlled; they shall be changed and distributed in accordance with established processes.

6.1.4 Hazard Analysis Tracking Index (HATI) (*NPR 8715.3*)

The HATI provides a way to track the status of hazard resolution and is merely a continuation of the FHA. The FHA data sheets provide the framework for the HATI. Its purpose is to verify that all the recommendations of the FHA have been implemented and all hazards have been eliminated, accepted, or closed as indicated in the status column of the analysis tables. Hazards identified through other techniques (e.g., failure modes and effects analysis (FMEA)) are also added to HATI for tracking. Use of the HATI starts in the construction phase because this is the first phase in which hazards can be field verified for closure, and it is updated throughout the project life cycle. The field inspection and verification is important to ensure that the safety controls have actually been put into place.

6.1.5 Facility Configuration Management Process (*NPR 8715.3, paragraph 8.3; and GLP–FB–8820*)

A configuration control process shall be in place to meet the requirements of NPR 8715.3C, paragraph 8.3. This requirement covers facilities at any phase of acquisition through operations and disposal. The configuration control process is a key element of system safety and change management. It ensures that the current systems are represented correctly on drawings and documents, which is imperative for operational and safety maintenance activities. It provides for proper documentation of design or facility changes and for all safety activities. The configuration control procedure shall require evidence of a proper safety review for any proposed modifications as well as prestartup safety reviews. This is especially critical for systems not covered by area safety committees or prior to safety committee involvement. At GRC the configuration control process is defined by GLP–FB–8820, Configuration Control of Facilities.

6.2 New Facilities and Systems (*NPR 8715.3*)

Figure 6.1 shows the GRC Facility System Safety Program as it relates to new facilities shall be integrated into the typical CoF project life cycle.

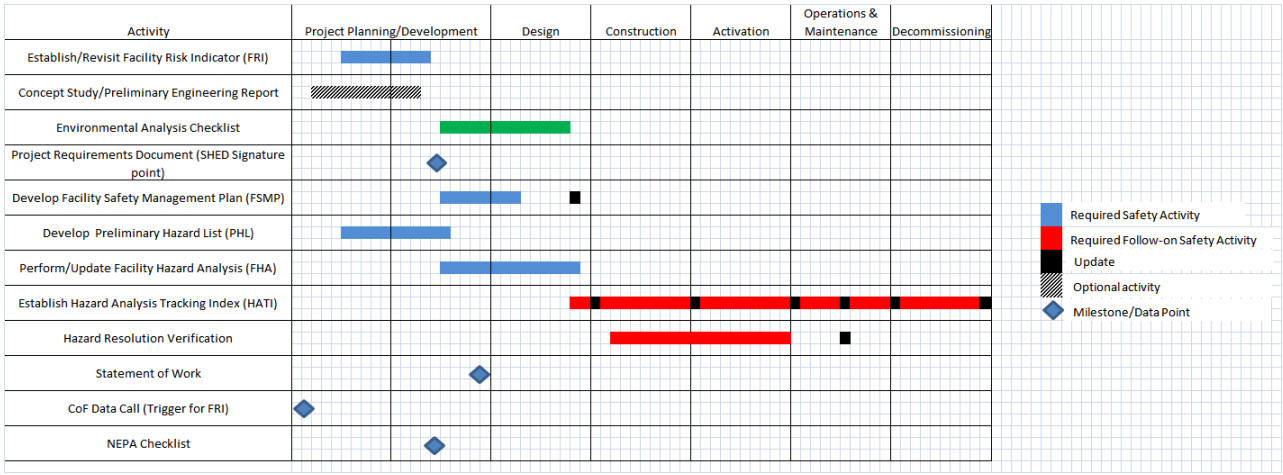

Figure 6.1.—GRC Facility System Safety Program activities.

6.3 Existing Facilities and Systems (*NPR 8715.3*)

For existing facilities, the items listed in Section 6.3 shall be performed as part of an ongoing process. The FRI will be determined for all facilities and the results will be used to prioritize which facilities will undergo the development of PHL and FHA independent of a project framework. Development and maintenance of FSMPs will be the responsibility of the Facility Manager.

6.4 Facility Hazard Analysis Preparation (*NPR 8715.3*)

The organization responsible for the facility to be modified or constructed shall assign someone to be responsible for the preparation of a FHA. The actual preparation should be performed by a team of NASA employees and/or support contractors. The following definitions provide a uniform understanding of the terms related to FHA preparation:

- Hazard description.—identifies the energy source that generates the hazard
- Cause.—describes those items that create or significantly contribute to the existence of the hazard
- Effect.—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 following sections describe the structure and content of a typical FHA.

6.4.1 Facility Hazard Analysis Organization

The FHA is divided into three main sections: introductory matter, text, and analysis tables. A critical items list (CIL) may be incorporated if the facility contains a critical item. The text is further subdivided into subsections common to all facilities although, on a case-by-case basis, additional special-item subsections can be added. The common subsections of the text are the introduction, the facility description, and the safety analysis summary.

6.4.1.1 Introductory Matter

The introductory matter consists of the title page, revision record, list of page revisions, and table of contents.

The title page contains the report title, the name of the facility for which the report was completed, the building number in which the facility is housed, and the FRI associated with the facility. The table of contents lists the major subsections of the FHA and the page number on which each begins. The revision record reflects all changes to a FHA; who prepared, reviewed, and accepted the report/changes and the date it was issued. The required signatures are as follows:

- The “Prepared By” area shall be signed by the individual who prepared the report or change.
- The “Reviewed By” area shall be signed by the designated reviewing authority.

- The "Reviewed By Safety Representative" area shall be signed by a safety professional assigned by SHeD.

NOTE: *Other signatures may be added to include other team members (e.g., project management).*

6.4.1.2 Text

The text section of the FHA consists of the introduction, the facility description, and the safety analysis summary. The introduction identifies the facility, states the purpose and philosophy of the analysis, and explains the risk assessment logic. The facility description provides a brief overview of the subject facility and describes the major facility capabilities, the nature of research conducted, the subsystems, and any special facility features appropriate to the safety analysis. It also includes a facility block diagram that shows the general relationships among the various subsystems. The safety analysis summary contains two sections, as follows

- General observations and recommendations.—addresses the hazards that are general in scope as opposed to specific to a particular subsystem and documents any other fact the FHA preparer feels is relevant
- Tabular summary.—presents a synopsis of the safety analysis of each major subsystem, which is given in detail in the analysis tables (Each hazard shall be assigned a risk level in accordance with the philosophy and guidelines established in Section 6.5)

6.4.1.3 Safety Analysis

The safety analysis of the FHA provides a detailed discussion of the hazards and risk assessments. There is typically a separate analysis table for each major subsystem identified on the facility block diagram.

6.4.1.4 Critical Items List (CIL)

The FHA includes a CIL for any facility that has a critical item. A critical item is any item, the single-order failure of which would likely result in death or damage to equipment or property equal to or greater than $1 million. Section 6.4.1.4 provides more details about preparing a CIL.

6.4.2 Facility Hazard Analysis Phases of Preparation

- **Phase I**, **System Definition Phase**.—During this phase, the preparer uses facility-provided documentation to define the system. The facility is divided into manageable subsystems. Examples of such subsystems are high-pressure air, vacuum, model injection, cooling water, test section, nitrogen, and hydrogen. How these subsystems are identified in any given facility depends on the methodology used by the preparer in organizing the FHA to cover every aspect of the facility. For example, in one instance, the model injection component may be a separate subsystem; whereas, in another instance, it may be included as part of the test section subsystem. The important thing is to ensure that all components of the facility are analyzed. Also at this time, a facility block diagram is generated to show the interrelationships among the chosen subsystems.
- **Phase II**.—Fill out the analysis tables using the hazards identified in the PHL development effort. With input from the Facility or Project Team, the preparer adds detail to the FHA. The FHA ensures that a deductive approach is taken in the assessment of the safety implications of the facility and it documents that thought process. Details of how to perform an HA are provided in Section 6.4.3.
- **Phase III**, **CIL (if required)**.—With the subsystems and hazards defined, the preparer assembles a CIL. A critical item must have the design analyses, in-service inspection and preventive maintenance procedures, installation procedures, and nondestructive testing required to establish and maintain an acceptable probability of occurrence. The requirement for design calculations can be waived for critical items that are proprietary or part of a company's standard product line, providing that the item has been designed to industry consensus codes, a history of acceptable operations of the same or similar products is available, and the use is in compliance with the manufacturer's ratings and recommended applications.

  Examples of proprietary items that meet the design waiver criteria are large rotating machinery for wind-tunnel compressor or drive systems. Critical items listed in a FHA shall be tracked throughout their lifetime for compliance with design, maintenance, and inspection requirements. Pressure components that are standard product lines and built to national consensus codes or standards are not considered critical items.

However, these items are covered under GRC's pressure system recertification program to assure system integrity.

- **Phase IV**.—A complete FHA is ready for a SHeD review. SHeD conducts a thorough and independent review of the FHA. Once the preparer and SHeD agree that the FHA is complete, a final project team review is conducted. During this phase, the remaining members of the project team review the FHA.
- **Phase V**.—The FHA is published. After all of the issues are resolved and the FHA is prepared in final format, it shall be formally approved by SHeD and the approving authority. Finally, it shall be configuration controlled.

6.4.3 Hazard Analysis (HA)

The HA begins with a detailed exploration of each of the identified hazards that came out of the PHL development effort (e.g., hot surfaces). A team approach is highly recommended for this process.

The team establishes what could cause a hazard to occur, and these become the causes (e.g., personnel error). There could be one or multiple causes for the same hazard. The analyst then quantifies the effects of each hazard in terms of damage, injury, and/or death (e.g., serious injury to personnel). When numerous effects result, only the most severe is noted.

To determine a facility's ability to avoid the occurrence of a hazard or limit the severity of an effect, the team assesses all safeguards including safety devices, instrumentation, procedures, and facility construction. This assessment takes the form of an investigation of the design and operational features that reduce the probability of each individual cause from occurring. In the interest of plausibility, the hazards, causes, and effects are to be confined to credible, as opposed to conceivable, events. They should reflect only those things that could reasonably be expected to occur.

6.4.4 Risk Assessment

The next step in the analysis is the risk assessment. An individual assessment is made and a risk assessment code (RAC) is assigned to each of the identified causes, using the guidance provided in Section 6.4.4.4. If an assigned risk assessment is unacceptable, as outlined in Section 6.4.4.4, recommendations are made that would reduce that risk assessment to acceptable limits if implemented. These recommendations can take the form of additional safety devices, design changes, or changes in the SOP.

An alphanumeric risk level, based on bot severity and probability of occurrence, shall be assigned to each cause of a hazard. The following paragraphs address how those risk levels are converted into a RAC using GRC's risk matrix.

6.4.4.1 Severity Category

A severity shall be assigned to each hazard, assuming it will occur. In this analysis, the worst possible result is to be assumed with no consideration being given to abatement techniques incorporated in the system design or to the use of procedures. The severity category provides a relative measure of the worst possible consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, and subsystem or component failure/malfunction. Table 6.1 lists the severity categories.

TABLE 6.1.—SEVERITY CATEGORIES

Category	Personal illness or injury	Equipment loss, $K	Downtime	Data integrity	Environmental effect
I (catastrophic)	Death	>1000	>4 months	Data never recoverable or primary program objectives lost	Long-term (>5 years) environmental damage or requiring >$1 million to correct and/or in penalties

II (critical)	Severe injury or occupational illness	1000 to 250	4 months to 2 weeks	Repeat test program	Medium-term (1 to 5 years) environmental damage or requiring $250,000 to $1 million to correct and/or in penalties

TABLE 6.1.—SEVERITY CATEGORIES

Category	Personal illness or injury	Equipment loss, $K	Downtime	Data integrity	Environmental effect
III (marginal)	Minor injury or occupational illness	250 to 25	2 weeks to 1 day	Repeat test period	Short-term (<1 year) environmental damage or requiring $25,000 to $250,000 to correct and/or in penalties
IV (negligible)	No injury or illness	25 to 1	<1 day	Repeat data point or data requires minor manipulation or computer rerun	Minor environmental damage, readily repaired, and/or requiring $1000 to $25,000 to correct and/or in penalties

6.4.4.2 Probability of Occurrence Level

A probability of occurrence shall be assigned to each cause of a hazard. The probability of occurrence provides a measure of system safety by evaluating the system design in conjunction with abatement techniques, inspections, tests, and operating procedures. The probability of occurrence is the probability that a failure will occur sometime during the planned life of the system. The probability level shall be qualitatively based upon engineering judgment with appropriate guidelines. Table 6.2 explains those guidelines.

TABLE 6.2.—PROBABILITY OF OCCURRENCE GUIDELINES

Level	Descriptive word	Qualitative definition	Quantitative definition
A	Frequent	Likely to occur repeatedly in system/component life cycle	$x > 10^{-1}$
B	Probable	Likely to occur several times in system/component life cycle	$10^{-1} \geq x > 10^{-2}$
C	Occasional	Likely to occur at sometime in system/component life cycle	$10^{-2} \geq x > 10^{-3}$
D	Remote	Not likely to occur in system/component life cycle, but possible	$10^{-3} \geq x > 10^{-6}$
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced	$10^{-6} \geq x$
F	Impossible	Occurrence is physically impossible	

6.4.4.3 Establishing a Risk Assessment Code

First, the effect of a hazard is evaluated in terms of severity (I, II, III, or IV). Next, the probability of occurrence (A, B, C, D, or E) is determined for each cause of the hazard. Using the severity of the hazard, each cause is assigned its own unique alphanumeric risk level (e.g., IA, IIB, or IIIC). Finally, using the two-dimensional risk matrix, each risk level is translated into a RAC (RAC 1, RAC 2, RAC 3, etc.). In Table 6.3, RAC 1s include blocks IA, IB, and IIA. RAC 2s include blocks IIB, IIIA, and IC. All other blocks are RAC 3s or higher.

TABLE 6.3.—RISK LEVEL MATRIX

Risk assessment code (RAC)	A frequent	B probable	C occasional	D remote	E improbable
I (catastrophic)	1	1	2	3	4
II (critical)	1	2	3	4	5
III (marginal)	2	3	4	5	6
IV (negligible)	3	4	5	6	7

6.4.4.4 Implications of a Given Risk Assessment Code

A RAC is a measure of the severity of a hazard versus the probability that the event will occur. As such, its value has implication of what shall be done prior to operation of a facility.

Table 6.3 shows RAC 1 and RAC 2 are the most serious of the levels of risk assessment. Accordingly, it is in the

best interest of all concerned to eliminate them through redesign, safety devices, special operating procedures, or combinations of such methods. The implications of the RACs shall be listed with the hazards analysis documentation in the FSMP. An example is given below.

- RAC = (1 or 2): unacceptable risk.—The operation cannot go forward without further hazard mitigation.
- RAC = (3): undesirable risk.—Director of Safety and Mission Assurance Directorate must review and approve.
- RAC = (4, 5, 6 or 7): acceptable risk.—This RAC is suitable for the project to review and accept the risk in conjunction with the cognizant safety authority (SHeD or area safety committee). Acceptance of the risk associated with these hazards is acknowledged by signing the FHA.

6.5 Glenn Research Center Interlock Philosophy

To conduct business at GRC, large power sources, pressurized gases, vacuums, hazardous materials, heavy machinery, and many other potentially dangerous conditions are present. The integration of safety into such an operation ensures the protection of the community, operating personnel, equipment, and the environment.

GRC's cornerstone strategy to achieve safety is its interlock philosophy, which is described below.

- A credible single-order failure that can jeopardize personnel or major equipment requires an interlock or protective device to prevent its occurrence. A safety interlock or protective device must be independent of the failure mode and cannot be compromised by occurrence of the credible single-order failure.
- When an independent safety interlock or device cannot be provided because of the utilization of a common component or path, then an independent component and/or path is necessary (e.g., hardwired backup of a software safety interlock or device).
- The safety interlock or device, unless it is verified automatically during startup (as a permissive), shall be periodically verified for operation. Period of performance shall be established by the safety analysis and specified in the FHA.
- Safety interlocks and devices, either software or hardware, must be under configuration control at the project level both before and during shakedown. Commencing at the operational readiness review (ORR), these safety interlocks and devices shall come under CM. At no time shall software changes be made while the facility is online (in operation).
- Forcing of safety interlocks or devices during facility operation (temporary changes to complete a run or to troubleshoot a problem) must be in accordance with an approved procedure and must have the permission of the SHED chief or a designated alternate.
- Failures of catastrophic proportions identified by the FSMP shall be assessed individually in the safety analysis and redundant safety interlocks or devices provided.

The above philosophy must be pursued regardless of the type of process control or complexity of the research facility. Several techniques can be used to achieve these aims to permit the necessary research to be accomplished. These techniques are discussed in the following paragraphs, in order of effectiveness, beginning with the most effective.

6.5.1 Design

The first line of safety is the initial design of a facility. Safety and interlock policies must be of equal and simultaneous consideration with research aims in the initial design phase of a facility. It is at this point that the best and the most cost-effective safeguards can be incorporated into a system.

6.5.2 Engineered Safety Features

Once a facility is constructed, additional safety margins can be attained by ad hoc engineered safety features. Such devices are an integral, permanent part of the facility and its routine operation. Like design features above, they are to be passive in nature and require no special action to cause them to be effective.

6.5.3 Safety Devices

Adjunct devices, such as goggles, hard hats, and safety bars, enhance safety. However, they require a conscious act on the part of the operator to become useful. Although they may appear cost effective, their effectiveness is moot if they are not employed.

6.5.4 Warning Devices

Visual and audible means to alert personnel to hazards are economical, but they are not barriers. Many of the techniques in the previous paragraphs are barriers. The term "barriers" implies that such devices prevent the occurrence of hazards. Warning devices are effective only when personnel are aware of them in sufficient time to react; and do, in fact, react.

6.6 Training

The introduction of the human element into a perfectly designed and controlled hardware system brings with it a potential for unexpected results. To minimize the occurrences of operator errors, a thorough training program shall be written and verified. If operator training and procedure compliance are to be completely effective in lowering the probability of hazards to an acceptable level, they must be coupled with some, if not all, of the foregoing abatement techniques.

Personnel involved in leading or reviewing hazard analyses for large projects or high-risk facilities (FRI of 1 or 2) or for multiple projects, shall take a course in hazard analysis or system safety. These classes provide instruction in various hazard methodology, hazard identification, and risk analysis. The NASA Safety Training Center (NSTC) offers two classes: SMA–SAFE–NSTC–0001, Facility System Safety, and SMA–SAFE–NSTC–0002, System Safety Fundamentals. Other comparable classes may be substituted.

7.0 RECORDS

The FSMP shall be maintained in a file by the Facility or Project Manager depending on project status. This includes all revisions of FHAs, FRIs, PHLs, and special documents used during the reviews. Specific revisions of drawings used and/or hand -marked notes to clarify the FHA texts are useful along with shutdown or alarm descriptions. The GRC Configuration Manager shall designate the recordkeeping requirements for all final true copies of the FSMP when the FSMP is approved by the Facility System Safety Committee.

8.0 REFERENCES

Document Number	Document Name
NPR 8715.3C	NASA General Safety Program Requirements
NPR 8820.2	Facility Project Requirements
NASA STD 8719.7	Facility System Safety Guidebook
GLP–FB–8820.1	Configuration Control of Facilities
GLM–QS–1700.1	Glenn Safety Manual, Chapter 1A, Glenn Safety Permit System

APPENDIX A.—DEFINITIONS AND ACRONYMS

Critical item.—Any item, the single-order failure of which would likely result in death or damage to equipment or property equal to or greater than $1 million.

Critical items list (CIL)

Configuration management (CM).—A field of management that focuses on establishing and maintaining consistency of a system's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life cycle.

Construction of facilities (CoF)

Facility.—Something that is built, installed, or established to serve a particular purpose and often comprises subsystems.

Facility change request (FCR)

Facility configuration management.—Establishes and maintains a baseline for designated systems (e.g., electrical systems) and the relevant documentation (e.g., drawings).

Facility hazard analysis (FHA).—A multistep, team-oriented approach to hazard and risk assessment that begins at the earliest phase of a project and continues throughout the life of the systems involved.

Facility life cycle.—Includes the design, acquisition, modification and test activities, operations and maintenance, and disposal of a facility.

Facility Manager.—Provides primary point-of-contact for the planning and scheduling of test programs and activities in the GRC test facilities. Provides the overall oversight and strategic management to ensure customers' requirements are satisfied and that the facilities are available and optimally utilized. Responsible for advocating, developing, scheduling, and maintaining the major GRC test facilities in a safe, reliable, and effective manner.

Responsible for the systems management, engineering development and commonality of the instrumentation, controls, and data acquisition systems in GRC test facilities.

Facility Safety Management Plan (FSMP).—The plan defining 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.

Failure modes and effects analysis (FMEA).—A procedure in operations management for analysis of potential failure modes within a system for classification by severity or determination of the effect of failures on the system.

Facility risk indicator (FRI).—Classifies the severity of potential hazards inherent to the facility itself: its operations, processes, environment, equipment, potential interfaces, and personnel.

Glenn Research Center (GRC)

Hazard.—A state or a set of conditions, internal or external to a system that has the potential to cause harm.

Hazard analysis (HA).—A process used to assess risk. The result of a hazard analysis is the identification of unacceptable risk and the selection of means of controlling or eliminating them.

Hazard analysis tracking index (HATI).—Part of the FHA, its purpose is to provide the user with a way to track the status of hazard resolution.

Hazard cause.—Describes those items that create or significantly contribute to the existence of the hazard.

Hazard description.—Identifies the energy source that generates the hazard.

Hazard effect.—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.

NASA Procedural Requirement (NPR) NASA Safety Training Center (NSTC) Operations Management Council (OMC)

Operational readiness review (ORR)

Plum Brook Management Office (PBMO)

Preliminary hazard list (PHL).—The purpose of the 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.

Probability of occurrence.—Probability that a failure will occur sometime during the planned life of the system.

Project Manager.—Individual responsible for the overall project from concept through completion, satisfying the project requirements, and who provides the primary interface with the customer or end user.

Risk.—Exposure to a chance of loss or damage or the combination of the hazard severity with the likelihood of its occurrence.

Risk assessment.—Consists in an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented.

Risk assessment code (RAC)

Safety analysis.—A systematic procedure for analyzing systems to identify and evaluate hazards and safety characteristics.

Safety, Health and Environmental Board (SHEB).—Serves as Glenn Research Center's safety, health, and environmental policy, and decisionmaking board. SHEB is responsible for the overall direction of the Center's safety, health, and environmental program.

Safety and Health Division (SHeD)

Standard (STD)

Standard operating procedure (SOP)

Subsystem.—Set of interacting or interdependent entities forming an integrated whole;examples of such subsystems are high pressure air, vacuum, model injection, cooling water, test section, nitrogen, hydrogen, and so forth.

Support service contractor (SSC)

APPENDIX B.—FACILITY RISK INDICATOR (FRI) EVALUATION

Approximately how many persons (contractors and civil servants) reside in your facility?

What is the primary function of your facility?

What programs/projects reside in your facility? (List major)

Could the loss of your facility have a serious impact on GRC's mission capability and/or operability? (Briefly explain)

APPENDIX B.—FACILITY RISK INDICATOR (FRI) EVALUATION CHECKLIST (CONTINUED)

A credible failure or mishap involving inherent hazards at your facility may cause (select one)

a. loss of life, permanent disability, or serious occupational illnesses to one or more persons

b. permanent disability to one or more persons

c. occupational injury or illness resulting in lost workdays or restricted duty

d. a first aid case

A credible failure or mishap involving inherent hazards at your facility may cause (select one)

a. damage to equipment or property in excess of $500,000

b. damage to equipment or property from $250,000 to $500,000

c. damage to equipment or property from $25,000 to $250,000

d. damage to equipment or property less than $25,000

A credible failure or mishap involving inherent hazards at your facility may cause (select one)

a. a loss of facility operational capability for 1 month or greater

b. a loss of facility operational capability from 2 to 4 weeks

c. a loss of facility operational capability from 1 day to 2 weeks

d. a loss of facility operational capability of less than 1 day

A credible failure or mishap involving inherent hazards at your facility may have an environmental impact to the adjacent facilities or operations or to the surrounding community resulting in (select one)

a. irreversible severe environmental damage that violates law or regulation

b. reversible environmental damage causing a violation of law or regulation

c. mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished

d. minimal environmental damage not violating law or regulation

Acoustical Radiation
- Equipment Noise
- Ultrasonic Cleaners
- Compressors

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

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)

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

Kinetic-Linear
- Cars
- Trucks
- Fork Lifts
- Carts
- Dollies
- Obstructions
- Shears
- Presses
- Crane Loads in Motion
- Pressure Vessel Blowdown
- Power Assisted Driving Tools

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

Propellant 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

Pressurized Systems
- Vessels (stationary or mobile)
- Cryogenic fluids

Electromagnetic and Particulate Radiation
- Radioactive Sources
- Waste and Scrap
- Contamination
- Irradiated Experimental and Reactor
- 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

Mass, Gravity, Height

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

Thermal (Except Radiant)

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

Notes:

APPENDIX C.—FACILITY SAFETY MANAGEMENT PLAN (FSMP) OUTLINE

I. Facility/system description

   A. Purpose, major systems, facility/system boundaries, general physical description

II. Facility risk indicator (FRI)

   A. Including: basis, supporting data, hazard list

   B. Periodic reviews of the FRI, facility hazards

III. Facility system safety organization

   A. Facility/System Manager

   B. Facility safety representative

   C. Center safety point of contact

   D. Center area safety committee with jurisdiction

   E. Facility/system engineer(s)

   F. Outline of responsibilities for the above

   G. Responsibilities relative to the facility safety program given below

IV. Facility System Safety Methodology

   A. Configuration management (CM) process

      1. References center CM programs and procedures as appropriate and lists specific or additional requirements.

      2. List specific design and safety review processes to be used depending on system type and status—ensure all required safety reviews are completed at the appropriate time (includes approval requirements)

         a) Center procedures for construction of facilities projects

         b) Facility change request procedures for facility or system changes

         c) Safety permit requests and change review for operational (test or research) systems including training requirements, scheduled maintenance of critical equipment, critical alarms, emergency shutdown systems and procedures

      3. Specific facility safety documentation process

   B. Hazard analysis process

      1. List of systems to be reviewed

      2. Type of review and schedule requirements

      3. Risk analysis methods

         a) Severity, probability, and risk codes (matrix) to be used

      4. Hazard Analysis Tracking Index (HATI)

         a) Verification/status of recommendations and approved mitigation

   C. Emergency plans

   D. Schedule of safety activities