Langley Procedural Requirements

LPR 1740.4 P
Effective Date: January 3, 2024
Expiration Date: January 3, 2029

Subject: Facility System Safety Analysis

Responsible Office: Safety and Mission Assurance Office

TABLE OF CONTENTS

LIST OF FIGURES

PREFACE

P.1 PURPOSE

This Langley Procedural Requirement (LPR) implements the requirements of NASA Procedural Requirements (NPR) 8715.3 and is part of the Langley Management System (LMS). This LPR sets forth procedural requirements for the Langley Research Center (LaRC) Facility System Safety Program for the Center's ground-based research facilities. It defines requirements for Facility System Safety Analyses and provides guidance for government and contract personnel in performing their responsibilities for this program.

P.2 APPLICABILITY

a. This LPR is applicable to all NASA LaRC organizations and all federal civil service personnel on Center.

b. This LPR is applicable to contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, agreements, or grants.

c. Noncompliance with the requirements of this LPR may result in appropriate disciplinary action against civil service personnel or sanctions against contractors in accordance with the terms of their contracts.

d. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

P.3 AUTHORITY

a. NPR 8715.3, NASA General Safety Program Requirements.

P.4 APPLICABLE DOCUMENTS AND FORMS

a. Who Must Follow the Regulations in Subchapter B?, 36 CFR § 1220.14.

b. What Types of Documentary Materials Are Federal Records?, 36 CFR § 1222.12.

c. NPD 1440.6, NASA Records Management.

d. NPR 7150.2, NASA Software Engineering Requirements.

e. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

f. NPR 8715.1, NASA Safety and Health Programs.

g. NPR 8715.3, NASA General Safety Program Requirements.

h. NASA-GB-8719.13, NASA Software Safety Guidebook.

i. NASA-STD-8739.8, Software Assurance and Software Safety Standard.

j. LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects.

k. LPR 1710.42, Safety Program for the Recertification and Maintenance of Ground-Based Pressure Vessels and Piping Systems (PVS).

l. LPR 1710.6, Electrical Safety.

m. LPR 1740.2, Langley General Safety Program Requirements.

n. LPR 1740.6, Personnel Safety Certification.

o. LPR 7123.2, Facility Configuration Management.

p. LMS-CP-4710, Facility Change Request Process.

q. LMS-CP-4754, Software Assurance (SA) for Development and Acquisition.

r. LMS-CP-7151, Obtaining Waivers for Langley Management System (LMS) Requirements.

s. LMS-CP-8715, Facility Risk Tier Determination.

t. LF 445, Facility Risk Indicator (FRI) Identification Form.

P.5 MEASUREMENT/VERIFICATION

None

P.6 CANCELLATION

LPR 1740.4L, dated March 9, 2018

_____

Title Date

Distribution: Approved for public release via the Langley Management System; distribution is unlimited.

CHAPTER 1: FACILITY SYSTEM SAFETY PROGRAM

1.1 INTRODUCTION

1.1.1 The Langley Research Center (LaRC) Facility System Safety Program exists to ensure the safe and continuous operation of ground-based LaRC facilities. It is composed of two major elements: safety analyses and Facility Configuration Management (FCM).

1.2 OBJECTIVES

1.2.1 The objectives of LaRC's Facility System Safety Program are to:

a. Ensure that the appropriate safety analyses are conducted.

b. Ensure that designated facilities/systems are placed under the appropriate level of facility configuration management based on the facility risk tier per LPR 7123.2. The risk tier for the facility is established by the Safety and Facility Assurance Branch (SFAB) using LF 445 (i.e., Facility Safety Personnel Listing (FSPL)) in accordance with LMS-CP-8715.

c. Document and communicate the risk of facilities and equipment to management and personnel.

1.2.2 The objectives of safety analyses, including a Facility System Safety Analysis (FSSA), are to:

a. Identify hazards,

b. Determine the risk of hazards in terms of severity and probability,

c. Assess the controls for those hazards, and

d. Recommend controls that will eliminate the hazard or reduce the risk of the hazard.

1.2.3 The objectives of a safety-critical software analysis are to:

a. Identify and document software hazards,

b. Assess the controls for those software hazards,

c. Recommend controls to mitigate hazards or reduce their risk outcomes, and

d. Ensure software risk mitigations and software hazard causations are duly considered during the FSSA.

Note: See NPR 7150.2 for the definition of software and related requirements.

1.3 WAIVERS

1.3.1 Requests for waivers to any of the requirements in this LPR shall be submitted to SFAB in writing and processed in accordance with LMS-CP-7151.

CHAPTER 2: FACILITY SYSTEM SAFETY ANALYSIS

2.1 PROGRAM SUMMARY

2.1.1 An FSSA is a systematic approach toward:

a. Identifying credible hazards associated with the operation of a facility,

b. Defining the hazards in terms of severity and probability,

c. Assessing the controls for those hazards,

d. Making recommendations toward reduction of the severity and probability of occurrence, and

e. Identifying documentation to place under facility configuration management control.

2.1.2 An FSSA shall be performed:

a. Prior to the start of research activities at a new facility,

b. Prior to the start of research activities at an existing facility that has undergone a Construction of Facility (CoF) modification, or

c. Prior to any existing facility being brought into the FCM Program.

2.1.2.1 FSSA Updates

2.1.2.1.1 FSSEs shall assess and update an existing FSSA for a facility in the FCM Program as appropriate to facility changes, facility condition, or other emergent safety concerns.

2.1.3 The final documents of this effort, all of which shall be placed in the FCM Program, are:

a. Standard Operating Procedures (SOPs) and Checklists,

b. Safety Analysis (e.g., Safety Analysis Report (SAR), Facility Operations Safety Hazard Analysis (FOSHA), or other hazard analysis as determined by the Facility System Safety Engineer (FSSE))

c. Configuration Controlled Items (CCIs),

d. Software Assurance Classification Reports (SACRs), and

e. Other items identified by the Facility Team.

2.1.4 The SAR documents the results of the FSSA. The remaining items support the FSSA and ensure hazard controls (e.g., procedures, interlocks) have been documented and placed under configuration control. This ensures the long-term safe operation of the facility.

2.1.5 The overall responsibility for conducting the FSSA lies with SFAB; however, the analysis is a group effort conducted by a Facility Team. A Facility Team may include:

a. Facility Manager (FM),

b. Facility Configuration Management Owner (FCMO),

c. Facility Systems Engineer (FSE),

d. Facility Safety Head (FSH),

e. Facility Coordinator (FC),

f. Facility Software Configuration Manager (FSCM),

g. FSSE from SFAB, and

h. Facility Software Safety Engineer (FSWSE) from SFAB.

2.1.6 The above members of a Facility Team are permanent members who also assist with meeting the requirements of the FCM Program. For new facilities or CoF projects, the Project Manager (PM) from the Project and Engineering Branch (PEB) is also a member of the Facility Team when an FSSA is conducted.

2.2 PLANNING AND EXECUTION

2.2.1 Existing Facilities

2.2.1.1 For an existing facility that will be added to the FCM Program or requires an update to an existing FSSA, the assigned SFAB FSSE shall notify the responsible FSH about the initiation of a FSSA.

2.2.1.2 The FSH, with the assistance of the facility staff, shall assemble and provide to the SFAB FSSE all existing documentation that reflects the “as-built" facility configuration. These documents include:

a. The appropriate facility electrical and mechanical drawings (redlined if necessary);

b. SOPs and checklists;

c. Vendor manuals, maintenance plans, and engineering reports/analyses; and

d. Any other item that may be of value toward the system safety analysis such as operational logs, failure mode histories, and specific areas of concern.

2.2.2 New Facilities, Facility Modifications, and CoF Projects

2.2.2.1 For new facilities, facility modifications, or CoF projects, the SFAB FSSE shall be involved during all phases of design, construction, and shakedown.

2.2.2.2 The FSH, with the assistance of the facility staff, shall assemble and provide to the SFAB FSSE all existing documentation that reflects the “as-built" facility configuration. These documents include:

a. The appropriate project electrical and mechanical drawings (redlined if necessary);

b. SOPs and checklists;

c. Vendor manuals, maintenance plans, engineering reports/analyses; and specification sheets, and

d. Any other item that may be of value toward the system safety analysis such as specific areas of concern.

2.2.2.3 At the start of any new project, the PM or FSH shall contact the SFAB FSSE, who will determine the scope required for the FSSA and initiate the analysis.

2.2.3 Details of how to develop a SAR and SOPs and identify CCIs are discussed in Sections 2.3-2.6. Details to develop the SACR and CCIs are covered in LPR 7123.2 and LMS-CP-4754.

2.3 SOP AND CHECKLIST DEVELOPMENT REQUIREMENTS

2.3.1 SOPs are detailed, written, formal instructions for certified operators to use during operation of the facility. Facility complexity and operational risks dictate the requirement for the degree of structured operations, which shall be controlled by SOPs and checklists.

2.3.2 This LPR establishes the requirements for developing, implementing, and updating SOPs into a standard format. With NASA LaRC facility/system-certified operators frequently being certified operators of several different facilities/systems, standard format SOPs are desirable in an effort to decrease the potential of an undesired event due to operator error.

2.3.3 This LPR shall be closely followed when developing SOPs for new facilities. Deviations from this instruction may be permitted to enhance clarity but shall require approval by the FSH, the FC, the FCMO representative, and SFAB.

2.3.4 It is not the intent of this LPR to require a rewrite of all existing SOPs. A total rewrite of SOPs for existing facilities could cause unnecessary confusion and may increase rather than decrease risk associated with facility operations.

2.3.5 The requirements to be followed in the preparation of SOPs are listed below:

a. SOPs shall provide for a complete cycle of operation (i.e., dormant to run and back to dormant). This cycle will be presented in three separate sections: Pre-operational Procedures (PR), Operational Procedures (OP), and Post-Operational Procedures (PO).

b. SOPs shall be developed in accordance with Appendix C of this LPR.

c. SOPs for the complete cycle shall be demonstrated and approved prior to being included in the FCM Program.

d. Initially, demonstrations shall be “dry runs” to avoid unnecessary exposure to hazards.

e. SOPs shall be approved by the FCMO, FSH, and SFAB representative.

2.3.6 Checklist Development Requirements

a. Checklists may be utilized by facilities to provide an avenue for certified operators to complete their work for routine, day-to-day operations of a facility.

b. Based upon the facility and the task to be performed by the certified operator, the checklist may take the form of:

(1) An abbreviated, one-to-one, less-detailed instruction of the SOP;

(2) An appendix to an SOP, which identifies a series of steps to be completed

before moving to the next step in the SOP (e.g., valve or circuit breaker line-up); or

(3) Routine facility tasks that do not require the level of detail offered by an SOP.

c. Checklists are not required; however, if a facility chooses to have checklists they must be demonstrated, approved, and brought under FCM prior to their use.

d. Checklists shall be developed in accordance with Appendix C of this LPR.

e. Checklists shall clearly identify the operations to be performed.

f. Checklists are often reproduced within the facility and a copy used for each operational run. In such cases, the entire checklist shall be reproduced and no part of the original omitted.

2.3.7 SOP/Checklist Organization

2.3.7.1 SOPs/checklists shall be divided into three sections: Introductory Matter, Text, and Emergency Procedures.

2.3.7.2 Introductory Matter

a. The Introductory Matter consists of the Title Page, Revision Record, General Introduction, and Safety Information.

b. The Title Page section shall contain the following:

(1) The SOP/checklist title.

(2) The name of the facility for which the document was completed.

(3) The building number in which the facility is housed.

(4) The statement *"THIS DOCUMENT CONTAINS HAZARDOUS OPERATIONS PROCEDURES."*

(5) The "Facility Owner/Supervisor" row shall be signed by the supervisor of the personnel who operate the facility or the director (or designee) of the facility.

(6) The "Facility Safety Head" row shall be signed by the FSH of the facility.

(7) The "SFAB Representative" row shall be signed by the appropriate SFAB FSSE assigned to the facility.

c. The Revision Record shall contain the date of issue, description of revision, and the pages affected.

d. A General Introduction page addresses the purpose, personnel, equipment, support and safety services, initial conditions, references, and remarks appropriate to the procedures/checklist being presented.

(1) Purpose: A short description of what the task/subtask(s) is to accomplish.

(2) Personnel: A listing of the minimum number of persons and their certification/qualification required to perform the task/subtask(s).

(3) Equipment: A list of the tools, test instruments, and the like needed to perform the task/subtask(s).

(4) Support and Safety Services: Identification of organizational elements and facilities required to support the operation (e.g., Air Control, Power Distribution, Safety, and Security).

(5) Initial Conditions: A description of assumptions made prior to beginning the task/subtask(s) (e.g., Pre-operational Procedures have been completed).

(6) References: Where to find other information needed for system operation.

(7) Remarks: Any information needed to clarify the task/subtask(s).

e. The Safety Information section contains information regarding any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation or use. The Safety Information section shall immediately follow the general introduction page and contain the following:

(1) Hazards: A statement for the certified operator(s) to refer to the Facility Resume, Hazard Analysis, SAR, or other applicable documentation for potential conditions that may be hazardous to personnel executing the procedure or to government property. Occupational hazards not listed in the facility SAR shall be listed here.

(2) Countermeasures: A statement for the certified operator(s) to refer to the Facility Resume, Hazard Analysis, SAR, or other applicable documentation for a list of hazard controls, including safety devices and interlocks, employed to reduce the risk to personnel or equipment from the hazards specified above.

(3) Hazardous Material(s): A statement for the certified operator(s) to see the Facility Resume, SAR, Hazard Analysis or Safety Data Sheet (SDS) Book, or to log into the Chemical Material Tracking System (CMTS) Log for a list of hazardous materials that may be encountered during execution of this procedure.

(4) Personal Protective Equipment: List the Personal Protective Equipment (PPE) required to safely and effectively accomplish the procedure.

2.3.7.3 Text

a. The Text section begins immediately following the Introductory Matter and consists of a sequence flow chart, which shows the safe order in which the PR, OP, and PO procedures can be executed, followed by the actual, step-by-step SOP/checklist.

2.3.7.4 Emergency Procedures

2.3.7.4.1 The Emergency Procedures section shall specify certified operator actions to be taken during an emergency in the location where the operational procedure is performed. Procedures in this section may include, but are not limited to, steps for emergency stop of the system(s) related to the corresponding SOP/checklist, personnel evacuation, injury and spill response, and listing of emergency contact information. The facility can use discretion in the level of detail necessary for this section. This section is

not intended to provide instructions on how to restore a failing system, but rather to ensure safety of personnel at the time the emergency occurs.

2.3.7.4.2 This section shall always be at the end of the SOP, regardless of any additional appendices used by individual SOPs.

2.3.8 Changes to SOPs/Checklists Developed Before LPR Effective Date

2.3.8.1 SOPs/checklists developed before the effective date of this LPR, requiring only an administrative change, shall not be required to be updated in accordance with the requirements set forth in this document.

2.3.9 SOPs/Checklists Changes and Distribution

2.3.9.1 SOPs/checklists are CCIs and as such they shall be changed and distributed in accordance with the requirements set forth in LPR 7123.2.

2.4 SAFETY ANALYSIS REPORTS (SARS)

2.4.1 A SAR is the formal documentation of the FSSA and shall be prepared in accordance with this LPR.

2.4.2 The SAR shall be a CCI and any change to the facility will be considered for possible SAR impact.

2.4.3 The SAR organizational structure detailed below are general guidelines that may be modified at the discretion of the FSSE dependent on the size and complexity of the system.

2.4.4 SAR Organization

2.4.4.1 The SAR is divided into three main sections – Introductory Matter, Text, and Appendices when applicable. The text is further subdivided into subsections common to all facilities although, on a case-by-case basis, additional special-item subsections (e.g., a Safety-Critical Items List) can be added. The common subsections of the text are the Introduction, the Facility Description, and the Safety Analysis Summary. The following is a discussion of each section.

2.4.4.2 Introductory Matter

a. The Introductory Matter consists of the Title Page, Revision Record, and Table of Contents.

b. The Title Page shall contain the following:

(1) The report title.

(2) The name of the facility for which the report was completed.

(3) The building or real property asset number in which the facility is housed.

(4) The Effort Code (EC) associated with the facility (if applicable).

(5) The “Facility Owner/Supervisor” row shall be signed by the Supervisor of the personnel who operate the facility or the director (or designee) of the facility.

(6) The “Facility Safety Head” row shall be signed by the FSH of the facility.

(7) The “SFAB Safety Engineer” row shall be signed by the appropriate SFAB FSSE assigned to the facility.

(8) The “LaRC Safety Manager” row shall be signed by the LaRC Safety Manager or designee.

c. The Revision Record shall contain the date of issue, description of revision, and the pages affected.

d. The Table of Contents lists the major subsections of the SAR and the page numbers on which they begin.

2.4.4.3 Text

a. The Text section of the SAR consists of the Introduction, the Facility Description, and the Safety Analysis Summary.

b. The Introduction identifies the facility, states the purpose and philosophy of the analysis, and explains the Risk Assessment logic.

c. 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.

d. The Safety Analysis Summary contains two sections: General Observations and Recommendations and Tabular Summary.

(1) The General Observations and Recommendations subsection addresses the hazards that are general in scope as opposed to specific to a particular subsystem and documents any other fact the analyst feels is relevant to the SAR but does not belong to any specific section of the document.

(2) The Tabular Summary subsection lists and discusses the identified undesired events and the associated risks. The Tabular Summary presents a synopsis of the safety analysis of each major subsystem, which is given in detail in the appendices. Each hazard/undesired event shall be assigned a risk level, before and after hazard controls are implemented, in accordance with the philosophy and guidelines established in Section 2.4.6.

2.4.4.4 Appendices

a. The appendices of the SAR provide a detailed discussion of the hazards, undesired events, and risk assessments. An appendix is necessary dependent on the size and complexity of the system as determined by the FSSE. There is a separate appendix for each major subsystem identified on the Facility Block Diagram.

2.4.4.5 Safety-Critical Items List

a. The SAR includes a Safety-Critical Items List for any facility that has a safety-critical item. Section 2.4.5.1 provides more details about preparing a Safety-Critical Items List.

2.4.4.6 SAR Changes and Distribution

a. SARs are CCIs, and as such, they shall be changed and distributed in accordance with the requirements set forth in LPR 7123.2.

2.4.5 SAR Preparation

a. The LaRC Safety Manager shall appoint a FSSE to be responsible for the oversight of the preparation of a SAR.

b. All SARs shall be reviewed and approved by the LaRC Safety Manager.

c. SAR preparation typically coincides with project phases as outlined in LAPD 7000.2 for new projects or facility modifications.

d. SAR development can be divided into four general phases: System Description, Hazard Analysis, Hazard Analysis Refinement, and Publishing. These phases are described below and summarized in **Figure *2-1***.

2.4.5.1 Phases

a. System Description Phase

(1) The system description phase begins at project conception and typically ends at the Preliminary Design Review (PDR).

(2) During this phase, the analyst will produce a description of the system, a description of each subsystem, and a preliminary hazard list associated with known energy sources.

(3) Prior to the PDR, the analyst will discuss the products with the project and facility team.

b. Hazard Analysis Phase

(1) The Hazard Analysis Phase begins after the PDR and ends at the Critical Design Review (CDR).

(2) This phase is an iterative process in which the analyst will analyze system hazards and mitigations and then generate a risk assessment with recommendations, as necessary.

(3) The risk assessment should be continuously reviewed and updated throughout this phase. An updated draft should be prepared prior to each design review.

c. Hazard Analysis Refinement Phase

(1) The Hazard Analysis Refinement Phase is an iterative process that begins after the CDR and ends at the Operational Readiness Review (ORR). The purpose of this phase is to update and finalize the hazard analysis. Any changes to the system during construction and testing shall be reflected in the final hazard analysis.

(2) Any changes to the system will be analyzed to determine if new undesired events are created and whether additional mitigations are necessary.

(3) During this phase, the analyst will establish and document a safety-critical

items list, as necessary.

(a) A safety-critical item shall have the design analyses, in-service inspection/preventive maintenance procedures, installation procedures, and nondestructive testing required to establish and maintain an acceptable probability of occurrence.

(b) With concurrence from the LaRC Safety Manager and COD Chief Engineer, the requirement for design calculations can be waived for safety-critical items that are proprietary or part of a company's standard product line, provided 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.

(c) Safety-critical items listed in a SAR shall be tracked throughout their lifetime for compliance with design, maintenance, and inspection requirements.

(d) Pressure components that are standard product lines and built to national consensus codes or standards are not considered safety-critical items; however, these items are covered under LaRC’s Pressure System Recertification Program to ensure system integrity per LPR 1710.40 and LPR 1710.42.

(4) The analyst will review the software-safety criteria no later than this phase. If the software is determined to be safety-critical, then the analyst will aid in the development of the software assurance classification report.

(5) At the end of each iteration, the analyst will review the information with the project and facility teams. The review is typically conducted prior to both the Integrated System Review (ISR) and the ORR but may be conducted additional times throughout this phase.

d. Publishing Phase

(1) Once a project is complete, the SAR shall be generated in accordance with the requirements in this LPR.

(2) Once the report is completed, it shall be submitted to the Facility Configuration Management System (FCMS) for approval and published as a CCI.

e. With the subsystems, hazards, and undesired events defined, the analyst prepares a Safety-Critical Items List.

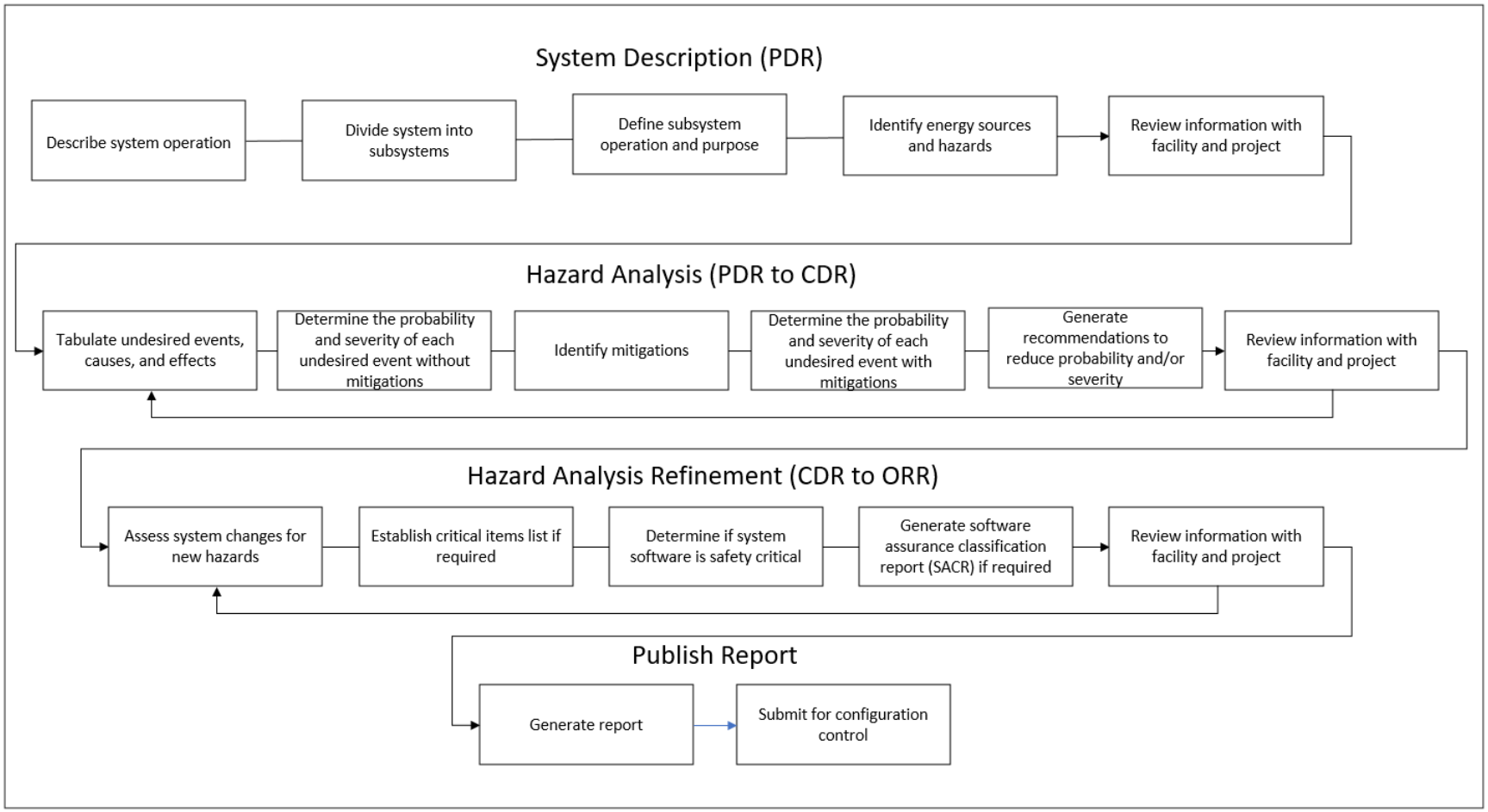

Figure 2-1. SAR Preparation Sequence

2.4.5.1.1 Hazard Analysis

a. The Hazard Analysis (HA) begins with a detailed exploration of each of the identified hazards (e.g., hot surfaces).

b. For each hazard, the analyst establishes what event(s) could occur that would result in the hazard causing injury (e.g., personnel in contact with hot surfaces), death, loss of major equipment, or damage to the environment. Those events become the undesired events. There could be multiple undesired events resulting from each identified hazard.

c. The analyst then quantifies the effects of each undesired event in terms of equipment damage, personnel injury and death, damage to the environment, or loss of productivity. When numerous effects result, only the most severe are noted.

d. Next, the analyst establishes what could cause an undesired event to occur, and these become the causes (e.g., personnel error). There could be one or multiple causes for the same undesired event.

e. The next step in the analysis is the risk assessment. An individual assessment is made without the consideration of any hazard controls in place to prevent the undesired event.

f. A Risk Assessment Code (RAC) is assigned to each of the identified causes using the guidance provided in Section 2.4.6.

g. To determine a facility's ability to avoid the occurrence of an undesired event, the analyst assesses the safety devices and procedures that are in place to minimize the probability of occurrence of each cause. This assessment takes the form of an investigation of the design and operational features that reduce the probability of each individual cause from occurring.

h. In the interest of plausibility, the undesired events, causes, and effects are to be confined to “credible” as opposed to “conceivable” events. They shall reflect only those things that could reasonably be expected to occur.

i. After the analyst has assessed the current hazard controls, the RAC is re-evaluated using the guidance provided in Section 2.4.6.

j. If an assigned RAC is unacceptable, as outlined in Section 2.4.6, recommendations are made, which would reduce that RAC to acceptable limits, if implemented. These recommendations can take the form of additional safety devices, design changes, or changes in the SOP.

2.4.6 Risk Assessment

2.4.6.1 LaRC uses a 5x5 risk assessment matrix to determine level of risk based on both severity and probability of occurrence. Risk levels shall be assigned to each cause of an undesired event before and after hazard controls are in place.

2.4.6.2 The following paragraphs address how those risk levels are converted into a RAC using LaRC’s risk matrix, which is depicted in **Figure *2-2***.

2.4.6.3 The effectiveness of a control is dependent on the undesired event. The risk assessment of the control is at the discretion of the analyst with the concurrence of the FSSE.

2.4.6.4 LaRC formerly utilized a 4x4 matrix to assess risk in each SAR. Existing SARs may continue to utilize the 4x4 matrix until a significant update is required, as determined by the analyst. The 4x4 matrix is illustrated in Appendix D. While there is not a one-to-one relationship between the risk assessment codes in the 4x4 and 5x5 matrices, the two may be translated by utilizing the category description tables of each (Appendix D for 4x4 matrix and **Table 2-1** and **Table *2-2*** for the 5x5 matrix).

2.4.6.5 Severity Category

2.4.6.5.1 A severity category shall be assigned to each undesired event assuming the event 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.

2.4.6.5.2 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 or malfunction. The Severity Categories are Minor, Moderate, Significant, Major and Catastrophic. Table 2-1 lists how severity is assigned based on the context of risk.

2.4.6.6 Probability of Occurrence

2.4.6.6.1 The probability of occurrence is the probability that a failure will occur sometime during the planned life of the system. 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. A probability of occurrence shall be assigned to each cause of an undesired event before and after hazard controls are in place.

2.4.6.6.2 The probability level shall be qualitatively based upon engineering controls, administrative controls, and any other supplemental data when available. The probability of occurrence categories are Very Low, Low, Moderate, High, and Very High. **Table *2-2*** illustrates how probability is assigned.

Table 2-1. 5x5 Matrix Undesired Event Severity Table

		Severity				
		1 (Minor)	**2 (Moderate)**	**3 (Significant)**	**4 (Major)**	**5 (Catastrophic)**
Safety	**Personnel**	Minor injury; Minor OSHA violation	Short-term illness or injury; moderate OSHA violation	Long-term illness or injury, impairment or incapacitation; significant OSHA violation	Permanent partial disability, injury, or incapacitation; Major OSHA violation	Loss of life or permanent total disability
	Facilities, Equipment, or Assets (NPR 8621.1)	Property damage of less than $20K	Property damage of >$20K but < $50k	Property damage of >50K but <$500k	Property damage of >$500k but <$2M	Property damage of >$2M
	Environment	Negligible EPA violation--non reportable	Minor reportable EPA violation	Moderate EPA violation that requires immediate remediation	Major EPA violation causing temporary stoppage	Serious or repeat EPA violations; termination of program
Performance	**Mission**	Minor impact to requirements, design margins, mission objectives, or exit criteria/performance goal of a milestone	Moderate impact to requirements, design margins, mission objectives, or exit criteria/performance goals of a milestone	Significant impact to requirements, design margins, mission objectives, or exit criteria/performance goals of a milestone	Major impact to requirements, design margins, mission objectives, or exit criteria/performance goals of more than one milestone	Technical goals not achievable with existing engineering capabilities/ technologies; failure to meet mission objectives
	Center Capabilities (Infrastructure & Workforce)	Minor impact to personnel, facilities, or infrastructure	Moderate impact to personnel, facilities, or infrastructure	Significant impact to personnel, facilities, or infrastructure	Major impact to personnel, facilities, or infrastructure	Catastrophic impact to personnel, facilities, or infrastructure

Table 2-2. 5x5 Matrix Undesired Event Probability Table

	Definition	Example Mitigations
5 (Very High)	Nearly certain to occur. Controls have little to no effect.	No engineering or administrative controls. Controls have little to no effect on mitigating hazard
4 (High)	Highly likely to occur. Controls have significant limitations or uncertainties.	Administrative Control
3 (Moderate)	May occur. Controls exist with some limitations or uncertainties.	One engineering control
2 (Low)	Not expected to occur. Controls have minor limitations or uncertainties.	One engineering control and an administrative control
1 (Very Low)	Extremely remote possibility that it will occur. Strong controls in place.	Redundant engineering controls or an engineering control with a sufficient administrative control

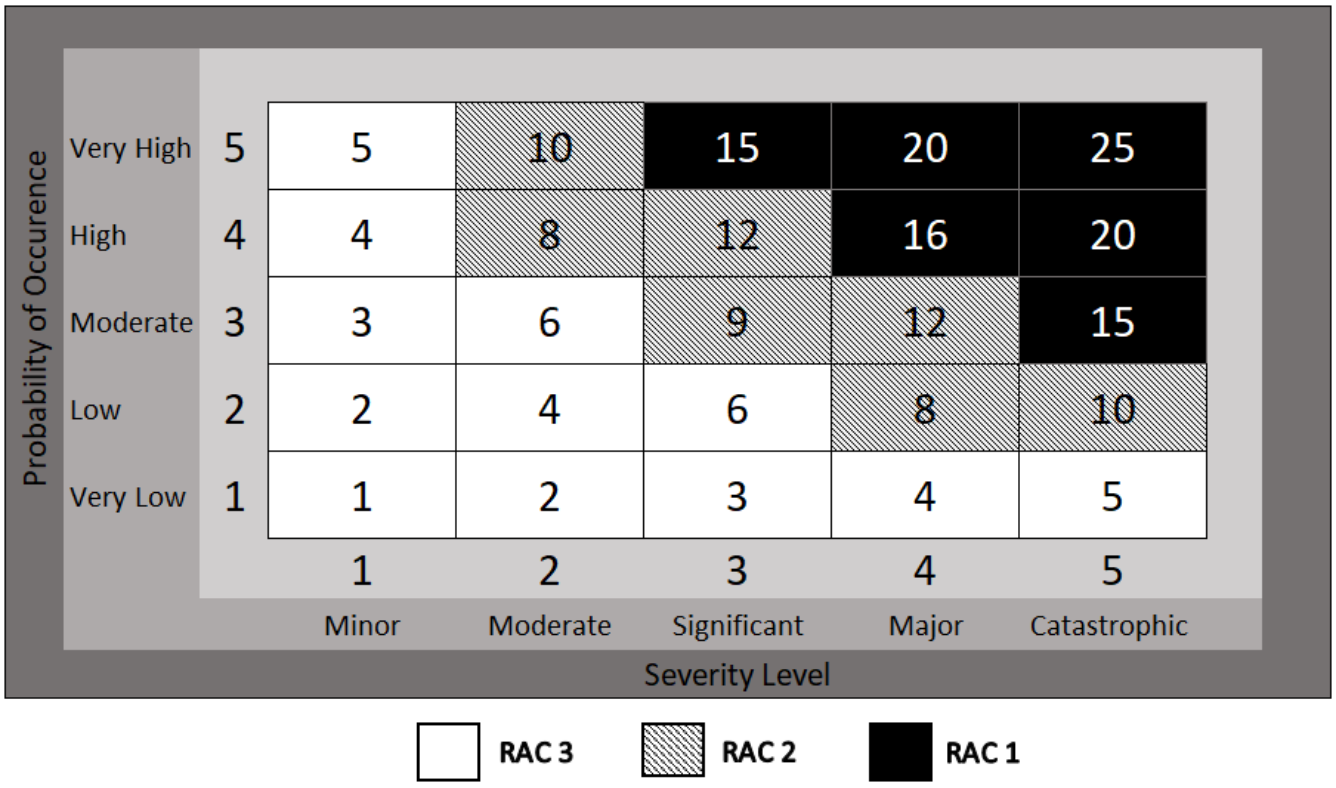

Figure 2-2. Risk Assessment Matrix

2.4.6.6.3 Establishing a Risk Assessment Code

a. First, the effect of an undesired event is evaluated in terms of severity (i.e., 1, 2, 3, 4, 5).

b. Next, the probability of occurrence (i.e., 1, 2, 3, 4, 5) is determined for each cause of the undesired event.

c. The assigned values for probability and severity are multiplied together to calculate the risk score (e.g., an undesired event with a probability of 3 and a severity of 2 would have a risk score of 3 x 2 = 6).

d. Each risk level is translated into one of three RACs based on the undesired event's assigned risk score: RAC 1 (risk scores 15, 16, 20, and 25), RAC 2 (risk scores 8, 9, 10, and 12), or RAC 3 (risk scores 1-6). The risk assessment matrix is shown in **Figure *2-2***.

Note 1: Undesired events can be referred to by their designated numeric probability and severity levels by stating probability followed by severity (e.g., 2x2, 3x4).

Note 2: As risk scores are calculated through multiplying the severity level by the probability level (both of which are 1 to 5), risk scores of 7, 11, 13, 14, 17, 18, 19, 21, 22, 23, and 24 are not possible.

e. After the in-place hazard controls are assessed, the above assessment is repeated using the newly established probability of occurrence.

2.4.6.6.4 Implications of a given RAC

a. As a RAC is a measure of the severity of an undesired event in relation to the probability that the event will occur, its score has implications regarding what is required to be done prior to operation of a facility.

b. RAC 1s are the most serious of the three levels of risk assessment. The implications of a RAC 1 are listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility.

(1) New/CoF Projects: RAC 1s associated with new facilities and CoF projects in existing facilities are of safety concern and require resolution (i.e., reduction of the RAC from 1 downward to 2 or 3) before the facility can initiate/resume operations.

(2) Existing Facilities, Systems, and Operations: RAC 1s associated with existing facilities not undergoing a major CoF are major safety concerns and require one of the following before the facility can resume operations:

(a) Resolution (i.e., reduction of the RAC from 1 to a 2 or 3), or

(b) An abatement plan approved by the LaRC Safety Manager, the director for the facility, the director for the personnel within the facility, and the Center Director.

Note: Failure to meet one of these requirements could result in facility shutdown.

c. RAC 2s are the second most serious of the three levels of the risk assessment. The implications of a RAC 2 are listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility. RAC 2s that have more than a minor increase to risk to personnel or a significant risk to property shall be approved by the Center Director in accordance with NPR 8715.1.

(1) New/CoF Project: RAC 2s associated with new facilities and CoF projects in existing facilities are also of concern and require special attention. Operations shall not begin in the facility until the chairperson of the final design review board, the LaRC Safety Manager, the director of the facility, and the director of the personnel within the facility have authorized operations to begin.

(2) Existing Facilities, Systems, and Operations: RAC 2s associated with existing facilities not undergoing a CoF require the approval of the director for the facility, the director for the personnel, and the LaRC Safety Manager before operations can resume. Plans and programs to correct existing RAC 2 undesired events, as time and resources permit, are considered sound management practice.

d. RAC 3s are at a risk level that needs to be accepted only by the SFAB FSSE, LaRC Safety Manager, and FSH. Acceptance of the risk associated with these undesired events is acknowledged by signing the SAR.

2.5 LARC HAZARD CONTROL STRATEGY

2.5.1 As part of routine business at LaRC, 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. LaRC's cornerstone strategy to achieve safety is its hazard control strategy, which is described below:

a. A credible single order failure that can jeopardize personnel or major equipment requires an interlock or protective device to prevent its occurrence.

b. 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.

c. When an independent safety interlock or device cannot be provided due to 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).

d. While not completely eliminating software safety risk, non-software hazard controls or mitigations (e.g., operator intervention, hardware backups/overrides, mechanical interlocks) can be used to mitigate software safety risk.

e. The safety interlock or device, unless it is verified automatically during startup as a permissive, shall be periodically verified for operation. The period of performance shall be established by the safety analysis and specified in the SAR.

f. Safety interlocks and devices, either software or hardware, shall be under

configuration control at the project level both before and during shakedown. Commencing at the ORR, these safety interlocks and devices shall come under the FCM Program in accordance with LPR 7123.2. At no time shall software changes be made while the facility is online (i.e., in operation).

g. Bypassing safety interlocks or devices during facility operation (e.g., temporary changes to complete a run or troubleshoot a problem) shall be in accordance with an approved procedure and have the permission of the FSH or a designated alternate.

h. Failures of catastrophic proportions identified by the FSSA shall be assessed individually in the safety analysis and redundant safety interlocks or devices provided.

2.5.2 The above strategy shall be pursued regardless of the type of process control or complexity of the research facility. In general, mitigations can be divided into two categories: engineered controls and administrative controls. The two categories and associated controls are discussed in the following paragraphs, in order of effectiveness, beginning with the most effective.

2.5.2.1 Engineered Controls are passive in nature and require no special action to cause them to be effective.

a. Design

(1) The first line of safety is the initial design of a research facility.

(2) Safety and interlock policies shall be of equal and simultaneous consideration with research aims in the initial design phase of a facility.

(3) It is at this point that the best and the most cost-effective safeguards can be incorporated into a system.

b. Interlocks

(1) A physical or software means to prevent conditions that cause undesired events

c. Safety Features

(1) 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.

(2) Barriers, relief valves and breakers are examples of safety features

2.5.2.2 Administrative controls require conscious action in order for them to be effective and are typically supplemental to engineered controls. Administrative controls are less effective than engineered controls but are often necessary for operations.

a. Personal Protective Equipment

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

b. Warning Devices

(1) 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 undesired events.

(2) Warning devices are effective only when personnel are aware of them in sufficient time to react; and do, in fact, react.

c. Procedures/Training

(1) The introduction of the human element into a designed and controlled hardware system brings with it a potential for unexpected results. To ensure that the occurrences of operator errors are minimized, a thorough training program shall be developed.

(2) The process shall be controlled by SOPs. If operator training and procedure compliance are to be effective in lowering the probability of an undesired event to an acceptable level, they must be coupled with some, if not all, of the foregoing abatement techniques.

2.6 CRITERIA FOR DESIGNATING CONFIGURATION CONTROLLED ITEMS (CCIs)

2.6.1 The hazard analysis is a detailed analysis that identifies hazards and the appropriate controls. This ensures the facility is safe at the start of operation, but it does not ensure a safety review of future changes to a facility. This is accomplished by designating the appropriate drawings, documents, and models (e.g., Building Information Models (BIM)) as CCIs and placing them in the FCM Program per LPR 7123.2.

2.6.2 CCIs are generally designated as such when they provide the following:

a. Support of the conclusions of the safety analysis or

b. Support the effective troubleshooting of systems (e.g., electrical, computer, mechanical).

CHAPTER 3: RISK AND SAFETY REVIEW

The risk and safety review aspect of the FCM Program consists of Facility Safety Reviews, procedure demonstrations, and continual Facility System Safety Analyses.

3.1 FACILITY SAFETY REVIEWS

3.1.1 Facility Safety Reviews are held for each LaRC facility. These meetings are scheduled at a frequency deemed appropriate by SFAB.

3.2 PROCEDURE DEMONSTRATIONS

3.2.1 Procedure demonstrations shall be conducted by a FCMO to validate the integrity of existing procedures. The following individuals shall be present during the procedure demonstration:

a. FSH,

b. FCMO,

c. Certified Operator(s), and

d. SFAB Representative.

3.2.2 Procedures that have not been verified or used within the last 12 months shall be verified by a procedure demonstration.

3.2.3 At the completion of a Procedure Demonstration, the FCMO representative shall notify all participants which procedures were demonstrated.

3.2.4 The FSH shall ensure any changes required based on the procedure demonstration are submitted via a Facility Change Request (FCR) per LMS-CP-4710.

3.3 CONTINUAL FACILITY SYSTEM SAFETY ENGINEERING ANALYSES

3.3.1 All configuration changes submitted by FCRs are subject to Facility System Safety Engineering Analyses by the designated SFAB FSSE. During this process, the FCM documents (e.g., SARs, SACRs, SOPs, checklists, and engineering drawings) are analyzed to assess the safety impact of the proposed changes.

APPENDIX A. DEFINITIONS

Cause. The stimulus or triggering mechanism/act that precipitates an undesired event.

Checklist. Utilized by facilities to provide an avenue for certified operators to complete their work for routine, day-to-day operations of a facility. Checklists are developed and maintained under the FCM Program.

Configuration Controlled Item (CCI). Facility baseline document, drawing, or engineering model (e.g., BIM) considered important to describing how a facility is configured, how it is to be operated, and what risks are associated with its operation. As such, CCIs are revised only through a formal change process under the FCM Program. Examples of CCIs include, but are not limited to, Safety Analysis Reports (SARs), Software Assurance Classification Reports (SACRs), SOPs and checklists, certain Pressure System Documents (PSDs), and selected engineering drawings.

Configuration Management (CM) Representative. Personnel supporting the LaRC FCM Program.

Effect. The consequence of an undesired event in terms of equipment damage, personnel injury/death, damage to the environment, or loss of productivity.

Effort Code (EC). A number that identifies a specific facility or group of facilities in the FCM Program. For the life of the facility, all CCIs will bear this number regardless of any facility name changes and/or hardware modifications.

Facility Coordinator (FC). An individual appointed to coordinate the overall day-to- day operations of a LaRC facility.

Facility Configuration Management Owner (FCMO). An individual appointed by the director with overall responsibility for ensuring configuration management of assigned facilities, labs, and systems.

Facility Configuration Management System (FCMS). A web-based server that enables users to access LaRC facility CCIs electronically via their desktop computer.

Facility Configuration Request (FCR). Prepared by the LaRC FCM Owner, FC, FSH, FSE, PM, or TPOC and processed by the Configuration Control Center (CCC.) The FCR is processed electronically via the FCMS. It is used in the LaRC FCM Program to request approval of and record all changes in the affected facility and to its supporting CCIs and integrated FCM disciplines (PSCM, CMMS, GIS, FSCM).

Facility Safety Head (FSH). An individual who ensures safe and efficient utilization of the facility in support of research programs internal and external to NASA.

Facility Software Configuration Manager (FSCM). A representative of the facility that supports the SCM activity for a particular facility.

Facility Software Safety Engineer (FSWSE). A representative of SFAB, SMAO, or a support contractor who participates in the development of the initial Facility System Safety Analysis, and/or an upgrade of an existing one, and supports the SCM activity for a particular facility.

Facility System Safety Analysis (FSSA). A continuing analysis throughout all phases

of the facility's life cycle involving the identification and control of hazards and the assessment of risks in operating that facility.

Facility System Safety Engineer (FSSE). A representative of SFAB, SMAO, or a support contractor who performs an initial Facility System Safety Analysis, and/or an upgrade of an existing one, and supports the CM activity for a particular facility.

Facility Systems Engineer (FSE). A representative of the facility, designated by the directorate who operates the facility, who performs system engineering analyses, and/or reviews existing analyses and supports the CM activity for the facility.

Facility Team. Personnel assigned to establish and prepare the CCIs for a LaRC facility during the initial Systems Safety Analysis or any subsequent upgrade effort. The team may include the FM, FCMO, FSE, FSH, FC, FSCM, SFAB FSSE, and SFAB FSWSE assigned to the System Safety effort and the Configuration Management Representative.

Field Verified (or Field Verification). The process by which the accuracy of a CCI or any other drawing is verified. That accuracy is attested to by affixing a "Field Verified" statement, signed by the person doing the verification, and signed and dated by the Project Engineer, FSH, or FC.

> *Note: For Field Verified (FV) or Field Verification relating to electrical work refer to LPR 1710.6*.

Hazard. A condition that has the potential to result in injury, death, loss of major equipment, or damage to the environment.

LaRC Safety Manager, SFAB, SMAO. This individual reviews and approves all Facility System Safety Analyses and reviews all changes to the SARs, SOPs, and checklists under the FCM Program.

Project Manager (PM). The engineer assigned to manage repairs, rework, or modifications to an existing research facility or construction of a new facility.

Redlining. The process of identifying changes on facility documentation by making color-coded annotations on the documents themselves. Deletions to be made are lined through with red markings; additions are shown in green ink or in black ink with yellow highlighting. Redlining of drawings may indicate proposed changes or changes to show the "as is" condition.

Research Facility (Facility). Ground-based apparatus or equipment directly associated with research operations, and sufficiently complex or hazardous to warrant special safety analysis and control.

Safety Analysis Report (SAR). A report under the control of the FCM Program that documents the formal Facility System Safety Analysis of a particular research facility.

Safety-Critical. Essential to safe performance or operation.

Safety-Critical Item. A safety-critical system, subsystem, condition, event, operation, or process that if not implemented or fails to perform as expected poses an unacceptable level of risk (e.g., RAC 1) to equipment and or personnel.

Safety-Critical Items List. A listing of safety-critical items for the affected facility.

Safety-Critical Software. Software is classified as safety-critical if the software is determined by and traceable to a hazard analysis. Software is classified as safety-critical if it meets at least one of the following criteria: a. Causes or contributes to a system hazardous condition/event; b. Controls functions identified in a system hazard; c. Provides mitigation for a system hazardous condition/event; d. Mitigates damage if a hazardous condition/event occurs; e. Detects, reports, and takes corrective action, if the system reaches a potentially hazardous state. Reference: NASA-STD-8739.8, *Software Assurance and Software Safety Standard*

Single Order Failure. A discrete system element or interface, the malfunction or failure of which, taken individually, would cause failure of the entire system.

Software Assurance Classification Report (SACR). A report under the control of the CM Program that documents the formal software assurance classification of a particular research system or facility.

Standard Operating Procedures (SOPs). Detailed, written, step-by-step instructions to be routinely followed in operating a facility. SOPs contain all of the information considered pertinent to safe and efficient operation of the facility. SOPs are the source documents for Operational Checklists and are the basis, in part, for the facility Hazard Control Analysis. SOPs may also be used for training certified operator personnel. SOPs are under the control of the FCM Program.

Undesired Event. An event (or series of events) that unleashes the potential inherent in a hazard and, either directly or indirectly, results in injury, death, loss of major equipment, damage to the environment, or loss of productivity.

APPENDIX B. ACRONYMS

BIM	Building Information Model
CCC	Configuration Control Center
CCI	Configuration Controlled Item
CDR	Critical Design Review
CM	Configuration Management
CMMS	Computerized Maintenance Management System
CMTS	Chemical Material Tracking System
CoF	Construction of Facility
COTS	Commercial-Off-the Shelf
CP	Center Procedure
EC	Effort Code
EPA	Environmental Protection Agency
FC	Facility Coordinator
FCM	Facility Configuration Management
FCMO	Facility Configuration Management Owner
FCMS	Facility Configuration Management System
FCR	Facility Change Request
FM	Facility Manager
FOSHA	Facility Operations and Safety Hazard Analysis
FRI	Facility Risk Indicator
FSCM	Facility Software Configuration Manager
FSE	Facility Systems Engineer
FSH	Facility Safety Head
FSPL	Facility Safety Personnel Listing
FSSA	Facility Systems Safety Analysis
FSSE	Facility System Safety Engineer
FSWSE	Facility Software Safety Engineer
FV	Field Verified
GIS	Geographic Information System
GOTS	Government-Off-the-Shelf
HA	Hazard Analysis

ISR	Integrated System Review
LAPD	Langley Policy Directives
LaRC	Langley Research Center
LF	Langley Form
LMS	Langley Management System
LPR	Langley Procedure Requirement
MOTS	Modified-Off-the-Shelf
NPR	NASA Procedural Requirement
OP	Operational Procedure
ORR	Operational Readiness Review
OSHA	Occupational Safety and Health Administration
PDR	Preliminary Design Review
PEB	Project and Engineering Branch
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
PM	Project Manager
PO	Post-Operational Procedure
PPE	Personal Protective Equipment
PR	Pre-Operational Procedure
PSCM	Pressure Systems Configuration Management
PSD	Pressure Systems Document
RAC	Risk Assessment Code
SACR	Software Assurance Classification Report
SAR	Safety Analysis Report
SCM	Software Configuration Management
SDS	Safety Data Sheet
SFAB	Safety and Facility Assurance Branch
SMAO	Safety and Mission Assurance Office
SOP	Standard Operating Procedure
TPOC	Technical Point of Contact

APPENDIX C. RECOMMENDATIONS FOR DEVELOPING SOPS/CHECKLISTS

C.1 INTRODUCTION

C.1.1 For the purpose of this LPR, SOPs are defined as detailed, written, formal instructions for certified operators to use during operation of the facility. SOPs are to include all tasks necessary to bring the facility/system from a dormant state or safe condition to an operational state and then return to a dormant state or safe condition.

C.1.2 Checklists that have been developed by abbreviating an SOP should have the SOP that was abbreviated listed on the title page of the checklist. SOPs that have had an abbreviated checklist developed to perform the same task should have the checklist listed on the title page of the SOP.

C.2 PRE-OPERATIONAL

C.2.1 The Pre-Operational section includes all activities required to bring systems/ subsystems from a dormant or safe condition to a condition ready for operation and may include pre-op maintenance and safety checks. This section can include list(s) such as a Valve List or a Circuit Breaker List. These list(s) describe the equipment condition or position required for proper facility/ system operation and may or may not require operator action for facility/system operation. These lists are intended to reduce the number of “verify” statements used in SOPs where equipment is normally left in the position needed for operation. The equipment list(s) may also provide a trouble-shooting guide that would be used to verify the proper condition or position for equipment in the event that the facility/system failed to operate.

C.3 OPERATIONAL

C.3.1 The Operational section includes all activities required during active operations of the facility/system. This also includes all activities required to turn around or re-cycle the facility/system for additional runs.

C.4 POST-OPERATIONAL

C.4.1 The Post-Operational section includes all activities required to bring the facility from an operational condition to a dormant or safe condition.

C.5 TASK AND/ OR SUB-TASKS

C.5.1 The complexity of the system dictates the detail and number of tasks and sub-tasks required. A flow sequence diagram is developed to provide a summary of the order in which tasks must be performed, at the facility safety head’s discretion.

C.5.2 The subdivisions of a document should be numbered in a way that reflects the organization of the document. This can be accomplished by: (a) assigning consecutive numbers to the major divisions of the document, beginning with 1 for the first, 2 for the second, and so on, (b) following this number with a period, (c) assigning consecutive numbers beginning with 1 to each subdivision, if any, of each major division and appending this number to that of the preceding division, (d) following this number with a period, and (e) continuing this process with any additional subdivisions until the

paragraph level is reached. The final number should not be followed with a period (e.g., 1. Introduction, 1.1 Safety Features, 1.1.1 Personal Protective Equipment).

C.6 LINE ITEMS OR STEPS

C.6.1 Line items or steps define actions that must be performed to accomplish a task or sub-task. Each facility/system has a logical, sequenced step-by-step order of actions that if performed as described will afford safe and reliable operation. The steps are to be presented in a chronological order and will be sufficiently detailed to permit a certified operator (per LPR 1740.6) to safely operate the facility/system. Each line item or step should be signed-off/initialed by the certified operator performing that step. Steps that have been deemed "Not Applicable" by a certified operator should be signed-off/initialed by the Facility Safety Head, including the date of the approval.

C.7 FLOW SEQUENCE DETERMINATION

C.7.1 The Sequential Flow Chart will specify a safe order for task performance that will result in reliable operation (, i.e., tasks and/or sub- tasks that can be performed concurrently or must be performed in sequence). The chart may vary extensively depending on the complexity of the facility/system. The facility team will discuss the Sequential Flow Chart with the certified operators of the facility/system to ensure proper flow. A single task procedure does not require a flow chart.

C.8 STANDARDIZATION

C.8.1 TASK IDENTIFICATION

C.8.1.1 Each task or sub-task should have an identification designation. An example of an identification designation for a Task or Sub-Task in a set of SOPs is 22-PR- 1-A. Each of the parts of the identification designation is defined below:

a. "22-" Identifies the facility/ system by EC number. This number is assigned by FCM Program.

b. "PR-" Identifies the task as a Pre-Operational Procedure (PR), an Operational Procedure (OP), or a Post-Operational Procedure (PO).

(1) Other supporting procedures may be utilized and their titles identified in this location. As an example, the National Transonic Facility (NTF) uses the following designations:

(a) AIP (Alarm/Alarm/Response Policy),

(b) IDSP (Instrumentation and Data System Procedure),

(c) IOP (Integrated Operating Procedure),

(d) MIP (Maintenance Instruction Procedure),

(e) MOP (Maintenance Operating Procedure),

(f) PMP (Preventative Maintenance Procedure), and

(g) SEP (Safety and Emergency Procedure).

c. "1-" Identifies the sequential flow task(s) of the SOP task and may be omitted if there is only one task. Generally, a series of tasks must be performed in order (i.e., PR-1 must be completed prior to the beginning of PR-2). Parallel listed

tasks are tasks that may not be required in every run condition and require the certified operator to determine which tasks should be performed for the particular run.

d. "A" Identifies sub-tasks (s) in the sequential flow of the SOP. The sub- task (s) may be done in any order but all sub-tasks (e.g., A, B, C) of a numbered task must be done before continuing to the next numbered task (i.e., PR-1-C may be done before PR-1-A, but all PR-1 tasks must be completed before beginning PR-2).

C.8.1.2 PAGE IDENTIFICATION

a. The Task Identification should be entered in the upper right-hand corner of each page.

b. Page numbers should be entered at the bottom center of each page.

c. Revision identification should be entered in the bottom right-hand corner (e.g., Rev. A).

d. The statement, "Configuration Controlled Item," should be entered at the top center of each page. Page number should be bottom, centered, and followed by revision right-justified. A mandatory statement, concerning requirement for use, should be at the bottom of the page and read as follows: "The procedural steps in this document are requirements and, as such, should not be deviated from without the express consent of the cognizant FSH."

C.8.1.3 STEP FORMAT

C.8.1.3.1 The following instructions are to be used when writing steps in the tasks or sub- tasks of SOPs. In unique or unusual circumstances, the facility team may deviate slightly from these instructions to enhance step clarity.

a. Steps that must be performed sequentially are to be identified numerically and must be performed in order (e.g., Step 1 must be completed before beginning Step 2, or Step 1.2 must be completed before beginning Step 1.3).

b. Steps that may be performed in any order are to be identified alphabetically (e.g., Step 3 (b) may be performed prior to or concurrently with Step 3 (a) at the discretion of the certified operator).

c. A step normally consists of three major entities: a command, the equipment commanded, and the final state and/ or reaction of the equipment.

d. The command should describe the action required to complete the step (e.g., verify, position, inspect). The command is to be written in lower case letters.

e. The equipment commanded will identify the switch, light, pushbutton, circuit breaker, disconnect switch, or component that is to be operated. If the equipment commanded has a label, the label should be entered into the step just as it appears on the control panel or piece of equipment and then underlined. The underlining of labels may be omitted if the team concurs that step clarity is enhanced.

f. The final state and/ or reaction of the equipment will be stated in capital letters (e.g., ILLUMINATED, EXTINGUISHED, CLOSED, OPEN). If the final state of the equipment is also the label on the equipment, then the label should be entered into the step as it appears on the equipment and underlined (e.g., “Position the switch to ON.” ON is the label on the switch). If the final state of the equipment is given in general terms and applies to a group of equipment, all capital letters may not be required (e.g., “Clear the test chambers of all personnel, close the test chamber door, and secure all dogs on the test chamber door.”).

g. The color of a light or component will have only the first letter capitalized (e.g., Green, Red, Clear).

h. Steps that identify a value to be recorded should identify the allowable tolerance for the recorded value.

i. Waivers should be requested in accordance with Section 1.3.

C.8.1.4 NOTES, CAUTIONS, AND WARNINGS

C.8.1.4.1 Notes, Cautions, and Warnings are used to delineate steps as follows:

a. NOTES may be used when all sequences in the steps cannot be clearly defined.

b. A NOTE is a step delineator; it is not a step replacement.

c. A NOTE may precede a step or series of steps in order to explain the required action.

d. A NOTE may be used to identify the location where a step is performed.

e. A NOTE may precede a step that, if performed erroneously, would invalidate previous system tests or acceptance.

f. A NOTE may precede a step that requires specific instructions.

g. A NOTE WILL NOT BE USED TO IDENTIFY HAZARDS TO PERSONNEL OR EQUIPMENT. SEE CAUTION AND WARNINGS BELOW.

h. A NOTE will be enclosed in the manner shown below:

NOTE

This operating procedure requires special emphasis for successful completion of the task

i. A CAUTION statement will precede any step or series of steps that if performed improperly, as defined in the safety analysis report, could damage equipment. A CAUTION statement will be enclosed in the manner shown below:

CAUTION

This operating procedure requires special emphasis for successful completion of the task

j. A WARNING statement will precede any step or series of steps that if performed

improperly, as defined in the safety analysis report, could endanger personnel. A WARNING statement will be enclosed in the manner shown below:

WARNING

This operating procedure requires special emphasis for successful completion of the task

C.8.1.5 CHECKLISTS

C.8.1.5.1 A checklist may be an abbreviated, one-to-one, less-detailed instruction of the SOP; an appendix to an SOP that identifies a series of steps to be completed before moving to the next step in the SOP (e.g., Valve or Circuit Breaker Line-up); or a list of routine facility tasks that do not require the level of detail offered by an SOP. The need for a checklist is a joint decision among the FSH, FC, and the Safety and Facility Assurance Branch. A checklist is not required for all facilities/systems; HOWEVER, if a checklist exists in an SOP, it must be CCI and used every time the facility/system is operated.

C.8.1.5.2 A checklist may be used to document system parameters required by research or as a tool that requires the certified operator to ensure that a level of operation is complete and the system is ready to continue to the next level of operation.

C.8.1.5.3 The following list further establishes instructions for generation of checklists:

a. A checklist is a CCI document and requires generation of a FCR for modification.

b. Checklist Format

(1) SOP steps that are included in a checklist are abbreviated to reduce verbiage and entered in the checklist.

(a) Example: The step in the SOP reads “Depress and Release the HYD. POWER lighted pushbutton and verify that the OFF light is EXTINGUISHED and the ON light becomes ILLUMINATED.” The step could be abbreviated in the checklist to “Start rotovalve hydraulic pump and verify ON light becomes ILLUMINATED.” in the checklist.

(2) WARNINGS in the SOP should be in the checklist and may be abbreviated to reduce verbiage as long as the meaning remains clear.

(3) CAUTIONS in the SOP should be in the checklist and may be abbreviated to reduce verbiage as long as the meaning remains clear.

(4) NOTES in the SOP that are only explanatory in nature may be included in the checklist at the facility’s discretion and also may be abbreviated to reduce verbiage as long as the meaning remains clear.

(5) Steps that identify a value to be recorded should identify the allowable tolerance for the recorded value.

(6) A checklist line item or step should be signed-off/initialed by the certified operator performing that line item or step.

(7) Mature systems may have “placard” type checklists that are conveniently posted at equipment to be operated.

c. Completed checklists are to be presented to, and retained by, the FSH. The period of time for retaining completed checklists will vary from facility to facility and is determined by the FSH, FC, and FM. The Safety and Facility Assurance Branch does not retain completed checklists.

Appendix D. 4x4 RISK ASSESSMENT MATRIX

D.1 Risk Assessment

D.1.1 LaRC formerly utilized a 4x4 risk assessment matrix to categorize the level of risk for each undesired event. The information contained within this appendix describes how risks are assessed utilizing the 4x4 matrix.

Note: The 4x4 risk assessment matrix has been superseded by the 5x5 risk assessment matrix and should not be used for new risk assessments.

D.1.2 An alphanumeric risk level, based on both severity and probability of occurrence, is assigned to each cause of an undesired event, before and after hazard controls are in place.

D.1.3 The following paragraphs address how those risk levels are converted into a RAC using LaRC's 4x4 risk matrix, which is depicted in **Figure D - *1***.

D.2 Severity Category

D.2.1 A severity category is assigned to each undesired event, 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.

D.2.2 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. The severity categories are Catastrophic, Critical, Marginal, and Negligible. **Figure D - *1*** includes guidance for assigning severity to undesired events.

D.3 Probability of Occurrence Level

D.3.1 A probability of occurrence shall be assigned to each cause of an undesired event before and after hazard controls are in place. 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.

D.3.2 The probability level shall be qualitatively based upon engineering judgment with appropriate guidelines. Those guidelines are Frequent, Occasional, Possible, and Remote. **Figure D - *1*** provides guidance for qualitatively assessing probability.

HAZARD SEVERITY

Hazard Severity Categories provide a relative measure of the worst possible consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system or component failure/malfunction, with no consideration given to abatement techniques. They are:

CATEGORY I - CATASTROPHIC. May cause death, permanent disability, the hospitalization of three or more people, and/or system/equipment damage in excess of $1,000,000.

CATEGORY II - CRITICAL. May cause lost time, injury or illness, and/or system/equipment damage between $250,000 and $1,000,000.

CATEGORY III - MARGINAL. May cause minor injury or illness and/or system/equipment damage between $1000 and $250,000.

CATEGORY IV - NEGLIGIBLE. Will not result in injury, illness, or system/equipment damage in excess of $1000.

HAZARD PROBABILITY

Hazard probability is the likelihood that a hazard will occur during the planned life expectancy of the system. The probability level is qualitative, based on engineering judgment, with appropriate guidelines as follows:

LEVEL A - FREQUENT. The level assigned when neither a safety feature nor approved procedures exist to prevent the undesired event from occurring.

LEVEL B - OCCASIONAL. The level assigned when a safety feature does not exist, but the use of approved procedures should prevent the undesired event from occurring.

LEVEL C - POSSIBLE. The level assigned when approved procedures do not exist, but an existing safety feature should prevent the undesired event from occurring.

LEVEL D - REMOTE. The level assigned when both a safety feature and approved procedures, or two independent safety features exist that collectively should prevent the undesired event from occurring.

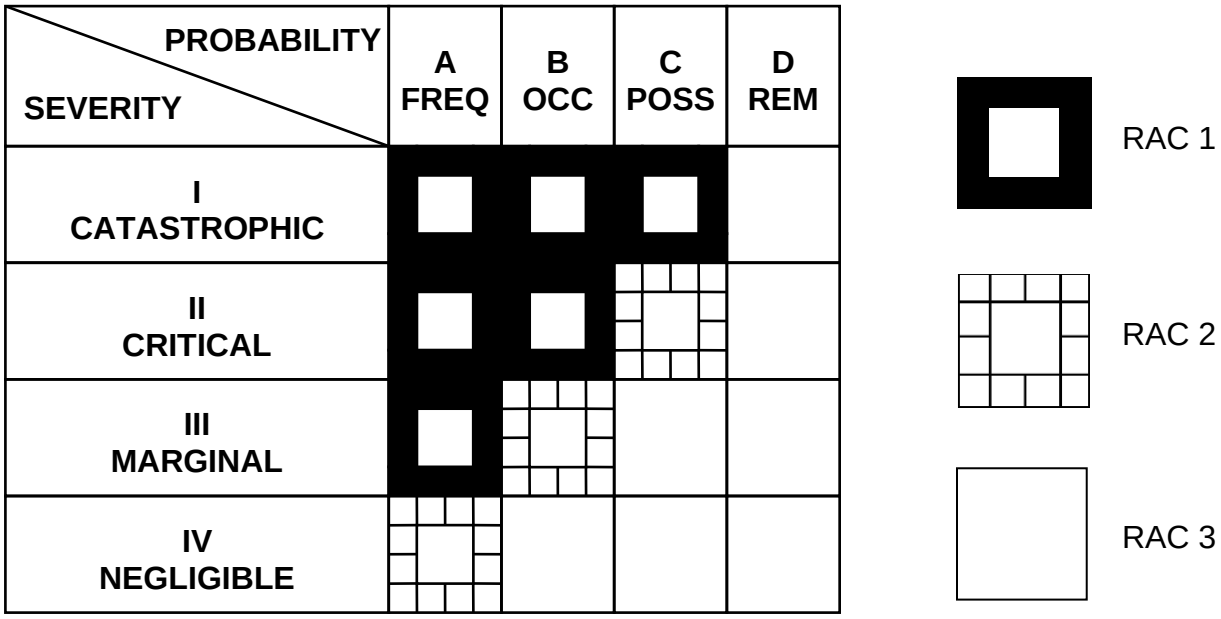

Figure D - 1. 4x4 Risk Assessment Matrix

APPENDIX E. RECORDS

E.1 All Federal personnel are required by law and Agency policy to maintain and preserve records. Documents listed in E.2 have been identified as meeting the statutory definition of Federal records as contained in 44 U.S.C. Section 3301, referred to in the National Archives and Records Administration (NARA) Regulations: 36 CFR Part 1220.14 and 1222.12, and NASA Policy Directive (NPD) 1440.6, “NASA Records Management.”

E.2 Identified documents:

a. Standard Operating Procedure(s)

b. Checklist(s)

c. Safety Analysis Report(s)