

**CENTER INTERIM DIRECTIVE**  
**CID (LPR) 1740.4, Facility System Safety Analysis**  
**and Configuration Management**

**Owning Organization: SMAO**

**Effective date: 8/19/2016**

**PLEASE NOTE:**

***These Langley Procedural Requirements have been updated to comply with federal regulations. Changes to the following sections will take effect immediately:***

**2.4.1.e.** Standard Operating Procedures shall be approved by the Facility Owner/Supervisor, Facility Safety Head, and Safety and Facility Assurance Branch Representative.

**2.4.3.1.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 employee(s) 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 Safety Engineer assigned to the facility.

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

**2.5.3.1.b.** The Title Page section shall contain the following:

- 1) The Report title.
- 2) The name of the facility for which the report was completed.
- 3) The building number in which the facility is housed.
- 4) The Effort Code (EC) associated with the facility.
- 5) The "Facility Owner/Supervisor" row shall be signed by the Supervisor of the employee(s) who operate the facility or the organizational director (or designee) of the facility.
- 6) "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 Safety Engineer assigned to the facility.
- 8) The "LaRC Safety Manager" row shall be signed by the LaRC Safety Manager or designee.

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

***All other portions of this LPR remain in effect.***

*Please submit any questions or concerns to Grant Watson, Director,  
Safety & Mission Assurance Office, at [grant.m.watson@nasa.gov](mailto:grant.m.watson@nasa.gov).*



**Langley  
Procedural  
Requirements**

**CID (LPR) 1740.4N**

Effective Date: 8/19/2016

Expiration Date: 8/19/2017

---

**Langley Research Center**

**FACILITY SYSTEM SAFETY ANALYSIS  
AND  
CONFIGURATION MANAGEMENT**

**National Aeronautics and Space Administration**

**Responsible Office: Safety and Mission Assurance Office****TABLE OF CONTENTS**

<b>Chapter</b>	<b>Page</b>
<b>PREFACE .....</b>	<b>4</b>
P.1 Purpose .....	4
P.2 Applicability .....	4
P.3 Authority .....	4
P.4 Applicable Documents and Forms .....	4
P.5 Measurement/Verification.....	5
P.6 Cancellation .....	5
 <b>1.0 FACILITY SYSTEM SAFETY PROGRAM.....</b>	 <b>6</b>
1.1 Introduction .....	6
1.2 Objectives .....	7
1.3 Definitions .....	8
1.4 Waivers .....	8
 <b>2.0 FACILITY SYSTEM SAFETY ANALYSIS .....</b>	 <b>9</b>
2.1 Program Summary .....	9
2.2 Planning and Execution.....	10
2.3 SOPs and Checklists.....	10
2.4 SOP Development Requirements .....	11
2.5 Safety Analysis Reports (SARs).....	13
2.6 LaRC Interlock Philosophy .....	23
2.7 Criteria for Designating Documents and Drawings as CCDs .....	25
 <b>3.0 FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM .....</b>	 <b>26</b>
3.1 Program Summary .....	26
3.2 Change Control .....	26
3.3 Updating and Distributing CCDs .....	27
3.4 Types of Change .....	27
3.5 Configuration Control Documentation – Drawings .....	29
3.6 Facility Baseline List (FBL) and Supporting Facility Documents .....	32
3.7 Filing Systems for CCDs .....	32
3.8 Risk and Safety Review .....	33
3.9 Configuration Management On-Line .....	34
 <b>4.0 PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM) .....</b>	 <b>35</b>
4.1 Program Summary .....	35
4.2 Pressure Systems Document (PSD) .....	35
 <b>5.0 FACILITY SOFTWARE ASSURANCE AND CM.....</b>	 <b>37</b>
5.1 General .....	37
5.2 Program Overview .....	37

<b>6.0</b>	<b>LANGLEY RISK EVALUATION PROGRAM (LREP)</b> .....	<b>44</b>
6.1	Program Summary .....	44
6.2	Langley Risk Evaluations (LRES) .....	45
6.3	Langley Operating Procedures (LOPS).....	45
6.4	LRE and LOP Changes and Distribution .....	46

## **APPENDICES**

<b>A.</b>	<b>DEFINITIONS</b> .....	<b>47</b>
<b>B.</b>	<b>ACRONYMS</b> .....	<b>52</b>
<b>C.</b>	<b>FACILITY RISK INDICATOR (FRI)</b> .....	<b>54</b>
<b>D.</b>	<b>REQUIREMENTS FOR DEVELOPING SOPS/CHECKLISTS</b> .....	<b>57</b>
<b>E.</b>	<b>RECORDS</b> .....	<b>64</b>

## **LIST OF FIGURES**

<b>FIGURE 2-1</b>	<b>SAR Preparation Sequence</b> .....	<b>17</b>
<b>FIGURE 2-2</b>	<b>Risk Assessment Matrix</b> .....	<b>21</b>
<b>FIGURE 5-1</b>	<b>SACR Preparation Sequence</b> .....	<b>40</b>
<b>FIGURE 6-1</b>	<b>Equipment/Operations LREP Energy Source Levels</b> .....	<b>44</b>

## **PREFACE**

### **P.1 PURPOSE**

This Langley Procedural Requirement (LPR) implements the requirements of NASA Procedural Requirements (NPR) 8715.3C, "NASA General Safety Program Requirements (w/ Change 4 dated 7/20/09)" and is part of the Langley Management System (LMS). This LPR sets forth procedural requirements for the Langley Research Center (LaRC) Facility System Safety and Configuration Management (CM) Programs for the Center's ground-based research facilities. It defines the requirements of the Center's Facility System Safety Analysis and CM Programs. It also provides guidance for government and contract personnel in performing their responsibilities for these programs.

### **P.2 APPLICABILITY**

- a. This LPR is applicable to all Langley employees and contractors.
- b. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

### **P.3 AUTHORITY**

NPR 8715.3, NASA General Safety Program Requirements

### **P.4 APPLICABLE DOCUMENTS AND FORMS**

- a. 36 CFR Part 1220.14, NARA Federal Records
- b. 36 CFR Part 1222.12, NARA Creation and Maintenance of Federal Records
- c. NPD 1440.6, NASA Records Management
- d. NPR 7150.2, NASA Software Engineering Requirements, Appendix E. Software Classifications
- e. NASA-GB-8719.13, NASA Software Safety Guidebook
- f. NASA-STD-8719.13B, NASA Software Safety Standard
- g. 00-MSC-ECSUM, Effort Code Summary, CMOL
- h. LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects
- i. LPR 1710.42, Safety Program for the Recertification and Maintenance of Ground-Based Pressure Vessels and Piping Systems
- j. LPR 1710.6, Electrical Safety
- k. LPR 1740.2, Facility Safety Requirements
- l. LPR 1740.7, Process Systems Certification Program
- m. LPR 7150.2, LaRC Software Engineering Requirements

- n. LPR 8717.1, Job Hazard Analysis Program
- o. LMS-CP-4710, Configuration Management for Facilities
- p. LMS-CP-4890, Construction and Change Assurance for High Risk Facilities
- q. LMS-CP-7151, Obtaining Waivers for Langley Management System (LMS) Requirements
- r. LMS-OP-8715, Identifying Facility Potential Hazard Levels
- s. Langley Form (LF) 127, Change Notification Sheet (CNS)
- t. LF 445, LaRC Facility Risk Indicator (FRI) Identification Form

## **P.5 MEASUREMENT/VERIFICATION**

None

## **P.6 CANCELLATION**

LPR 1740.4N, dated November 11, 2015

<u>/s/ Clayton P. Turner</u>	<u>August 19, 2016</u>
Center Deputy Director	Date

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

## **CHAPTER 1.0 – FACILITY SYSTEM SAFETY PROGRAM**

### **1.1 INTRODUCTION**

1.1.1 The 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:

- a. Safety Analysis, which takes the form of either a:
  - 1) Facility System Safety Analysis (FSSA) or
  - 2) Langley Risk Evaluation (LRE)
- b. Configuration Management that includes:
  - 1) Facility Configuration Management (CM) Program,
  - 2) Pressure Systems Configuration Management (PSCM),
  - 3) Software Configuration Management (SCM),
  - 4) Langley Risk Evaluation Program (LREP), and
  - 5) Computer System Inventory (CSI).

1.1.2 LaRC research facilities included in the Facility CM Program have been designated with a Facility Risk Indicator (FRI) of 1 (see Appendix C for details of FRI classification) and require a safety analysis conducted in accordance with the Facility System Safety Analysis process. The Safety Manager shall appoint a Safety and Facility Assurance Branch (SFAB) Facility System Safety Engineer (FSSE) to be the safety point of contact for each of these facilities.

1.1.3 Each research facility assigned an FRI 1 also has a unique number, called an Effort Code (EC), to aid in tracking configuration controlled documentation (CCD). The present FRI 1 research facilities and FRI 1 systems EC numbers are listed in the Configuration Management On-line (CMOL) program and may also be found in OP-8715, "Identifying Facility Potential Hazard Levels."

1.1.4 SFAB utilizes the FRI in determining whether a research facility or piece of research equipment is placed in the Facility Configuration Management Program, Langley Risk Evaluation Program, or under a Safety Permit. All research facilities at LaRC are given a FRI. The assessment criterion for assigning a FRI to a facility is located in Appendix C. Additions/Changes to FRIs and ECs numbers at LaRC shall be completed via a LF 445, Facility Risk Indicator (FRI) / Effort Code (EC) Change Request.

1.1.5 Details on the Facility System Safety Analysis process, LREP, and the various CM programs are found in the remainder of this document as described below:

- a. Chapter 2 addresses the FSSA process.
- b. Chapter 3 addresses the Facility CM Program.
- c. Chapter 4 addresses the PSCM Program.

- d. Chapter 5 addresses the Facility Software Assurance and SCM processes.
- e. Chapter 6 addresses the LREP.

## **1.2 OBJECTIVES**

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

- a. Ensure that the appropriate safety analysis has been conducted,
- b. Ensure that designated facilities/systems are placed under the appropriate level of configuration management, and
- c. Document and communicate the risk of facilities and equipment to management and employees.

1.2.2 The objectives of a safety analysis, whether a Facility System Safety Analysis or Langley Risk Evaluation, 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 the Facility CM program are to:

- a. Record and maintain safety analysis documentation,
- b. Document and maintain standard operating procedures for use by operating personnel,
- c. Ensure SFAB reviews changes that affect safety, and
- d. Establish and maintain a baseline for designated systems (e.g., electrical systems) and the relevant documentation (e.g., drawings).

1.2.4 The objective of the Pressure Systems Configuration Management Program is to maintain the configuration of Pressure System Documents (PSD).

1.2.5 The objectives of the Langley Risk Evaluation Program are to:

- a. Record and maintain the risk evaluation and
- b. Document and maintain Langley Operating Procedures (LOPs) for use by certified operating personnel.

1.2.6 The objectives of the Software Safety Planning Program are to:

- a. Evaluate software against NASA-STD-8719.13B to determine safety criticality,
- b. Establish a risk-profile for safety-critical computer systems,
- c. Identify all safety-critical computer systems,
- d. Estimate a software assurance effort for safety-critical software systems,



- e. Document the above steps via the Software Assurance Classification Report (SACR), and
- f. Complete a safety-critical software analysis.

1.2.7 The objectives of a safety-critical software analysis, whether part of an FSSA or LRE, are to:

- a. Facilitate the identification and documentation of software hazards,
- b. Help assess the controls for those software hazards,
- c. Recommend controls to mitigate hazards or reduce their risk outcomes,
- d. Ensure software risk mitigations and software hazard causations are duly considered during the FSSA or LRE.

1.2.8 The objectives of the Facility SCM Program are to:

- a. Document and maintain configuration control of software,
- b. Ensure SFAB reviews changes that affect safety, and
- c. Establish and maintain a baseline for designated systems (e.g., computer systems) and the relevant documentation (e.g., drawings).

### **1.3 DEFINITIONS**

1.3.1 The glossary in Appendix A lists and defines the terms unique to the Facility System Safety and CM Programs.

### **1.4 WAIVERS**

1.4.1 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, Obtaining Waivers for Langley Management System (LMS) Requirements.

## CHAPTER 2.0 – 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/or probability of occurrence, and
- e. Identifying documentation to place under configuration control.

2.1.2 A 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 Facility CM Program.

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

- a. Standard Operating Procedures (SOPs) and Checklists,
- b. Safety Analysis Report (SAR),
- c. Configuration Control Documentation (CCD),
- d. SACR, and
- e. Other special 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 the SFAB; however, the analysis is a group effort conducted by a Facility Team. A Facility Team includes:

- a. Facility Manager (FM),
- b. Facility Systems Engineer (FSE),
- c. Facility Safety Head (FSH),
- d. Facility Coordinator (FC),
- e. Facilities Configuration Coordinator (FCC) from the Project and Engineering Branch (PEB), Center Operations Directorate (COD),
- f. Facility Software Configuration Manager (FSCM),
- g. Facility System Safety Engineer (FSSE) from SFAB,
- h. Facility Software Safety Engineer (FSWSE) from SFAB, and

i. CM Representative.

2.1.6 The above members of a Facility Team are permanent members who also assist with meeting the requirements of the Facility CM Program. For new facilities or CoF projects, the Project Manager (PM) from the PEB is also a member of the Facility Team during performance of the FSSA.

## **2.2 PLANNING AND EXECUTION**

2.2.1 For an existing facility that will be added to the Facility CM Program, the assigned SFAB FSSE shall notify the responsible FSH about the initiation of a FSSA.

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-is" facility configuration. These documents include:

- a. The appropriate facility electrical and mechanical drawings (redlined if necessary),
- b. Draft SOPs and/or 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.

2.2.3 These documents form the foundation of the FSSE's formal analysis of the facility's hazards and other conditions appropriate to the issue of safety. Details of how to develop a SAR, SACR, and SOPs and identify CCD are discussed in Sections 2.3, 2.4, 2.5, 2.7 and 5.2.

2.2.4 For new facilities or CoF projects, it is very important that the SFAB FSSE be involved during all phases of design, construction, and shakedown. For these projects, the FSSA shall be an integral part of the design process as outlined in Paragraph 3.4.4, Change Controlled by Design Review Process.

2.2.5 At the start of any new project, the PM or FSH shall contact the SFAB FSSE, who will initiate the FSSA.

## **2.3 SOPs AND CHECKLISTS**

2.3.1 Instructions for the development of SOPs and checklists are found in the following paragraphs. Facility complexity and operational risks dictate the requirement for the degree of structured operations, which shall be controlled by SOPs and/or checklists.

## 2.4 SOP DEVELOPMENT REQUIREMENTS

2.4.1 SOPs are detailed, written, formal instructions for certified operators to use during operation of the facility. The requirements to be followed in the preparation of SOPs are listed below:

- a. SOPs shall provide for a complete cycle of operation (dormant to run 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 D, Requirements for Developing SOPs/Checklists.
- c. SOPs for the complete cycle shall be demonstrated and approved prior to being included in the CM Program.
- d. Initially, demonstrations shall be “dry runs” to avoid unnecessary exposure to hazards.
- e. SOPs shall be approved by the Facility Owner/Supervisor, FSH, and SFAB Representative.

### 2.4.2 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 for a facility in the CM Program; however, if a facility chooses to have checklists they must be demonstrated, approved, and brought under CM prior to their use.
- d. Checklists shall be developed in accordance with Appendix D, Requirements for Developing SOPs/Checklists.
- e. Checklists shall clearly identify what is included.
- 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.

### 2.4.3 SOP/Checklist Organization

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

#### 2.4.3.1 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 employee(s) 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 Safety Engineer 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 tasks/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 see the Facility Resume and SAR 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 see Facility Resume and SAR for a list of safety devices, interlocks, etc. 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, or Material Data Sheet Book or to log into the Chemical Tracking System 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.

#### 2.4.3.2 Text

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.

#### 2.4.3.3 Emergency Procedures

2.4.3.3.1 The Emergency Procedures section shall specify certified operator actions to be taken during plant emergencies (e.g., emergency contact information, routes of exit, fire alarms and extinguishers). This section is not intended to provide personnel with information to take a corrective action to restore a failing system or to attempt to control the source of the emergency.

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

#### 2.4.4 Changes to SOPs/Checklists Developed Before LPR Effective Date

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.

#### 2.4.5 SOPs/Checklists Changes and Distribution

Because SOPs/checklists are CCDs, they shall be changed and distributed in accordance with the requirements set forth in Chapter 3 of this document.

### 2.5 SAFETY ANALYSIS REPORTS (SARS)

2.5.1 A SAR is the formal documentation of the FSSA and shall be prepared in accordance with Section 2.5.2.

2.5.2 The SAR shall be a CCD document and any change to the facility will be considered for possible SAR impact.

### 2.5.3 SAR Organization

The SAR is divided into three main sections – Introductory Matter, Text, and Appendices. 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.

#### 2.5.3.1 Introductory Matter

- a. The Introductory Matter consists of the Title Page, Revision Record, and Table of Contents.
- b. The Title Page section shall contain the following:
  - 1) The report title.
  - 2) The name of the facility for which the report was completed.
  - 3) The building number in which the facility is housed.
  - 4) The Effort Code (EC) associated with the facility.
  - 5) The “Facility Owner/Supervisor” row shall be signed by the Supervisor of the employee(s) who operate the facility or the organizational director (or designee) of the facility.
  - 6) “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 Safety Engineer 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 number on which each begins.

#### 2.5.3.2 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) General Observations and Recommendations address the hazards that are general in scope as opposed to specific to a particular subsystem and document any other fact the FSSE feels is relevant to the SAR but does not belong in an appendix.
  - 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 an alphanumeric Risk Level, before and after hazard controls are implemented, in accordance with the philosophy and guidelines established in Section 2.5.4.

#### 2.5.3.3 Appendices

The appendices of the SAR provide a detailed discussion of the Hazards, Undesired Events, and Risk Assessments. There is a separate appendix for each major subsystem identified on the Facility Block Diagram.

#### 2.5.3.4 Safety-Critical Items List

The SAR includes a Safety-Critical Items List for any facility that has a safety-critical item. Section 2.5.4.1.g provides more details about preparing a Safety-Critical Items List.

#### 2.5.3.5 SAR Changes and Distribution

Because SARs are CCDs, they shall be changed and distributed in accordance with the requirements set forth in Chapter 3 of this document.

#### 2.5.4 SAR Preparation

- a. The Safety Manager shall appoint a SFAB FSSE to be responsible for the preparation of a SAR. The actual preparation is performed by either the SFAB FSSE or a FSSE from a support contractor.
- b. Any SAR prepared by a support contractor shall be reviewed and approved by the SFAB FSSE.
- c. The definitions Hazard, Undesired Event (UE), Cause, and Effect provide a uniform understanding of the terms related to SAR preparation. See Appendix A – Definitions.



#### 2.5.4.1 Phases

- a. The phases of SAR preparation are outlined in Figure 2-1, "SAR Preparation Sequence." A description of each phase follows.
- b. The first phase is the System Definition Phase. During this phase, the FSSE uses facility, provided documentation to define the system. The facility is divided into manageable subsystems (e.g., high pressure air, vacuum, model injection, cooling water, test section, nitrogen, hydrogen).
- c. These subsystems are identified in any given facility depending on the methodology used by the FSSE in organizing the SAR 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.
- d. Next, the FSSE performs a Preliminary Hazard Analysis (PHA) to identify all the possible hazards and undesired events that could result from those hazards. This phase represents an initial safety assessment of the facility. The hazards and undesired events established here will be expanded as the safety analysis progresses. There may be none or any number of hazards in each of the subsystems. Upon completion of this phase, copies of the products shall be sent to the Facility Team for initial review and clarification of the facility hazards and undesired events.
- e. Upon completion of the PHA the Initial Facility Team Review is conducted. The Facility Team conducts an initial review of the effort by examining the System Definition and Preliminary Hazard Analysis products and provides the FSSE additional information and comments.
- f. With input from the Facility Team, the FSSE performs a detailed Hazard Analysis (HA). The HA ensures that a deductive approach is taken in the assessment of the safety implications of the facility and it documents that thought process. The approach taken is reflected in Figure 2-1, "SAR Preparation Sequence." Details of how to perform an HA are provided in Section 2.5.3.

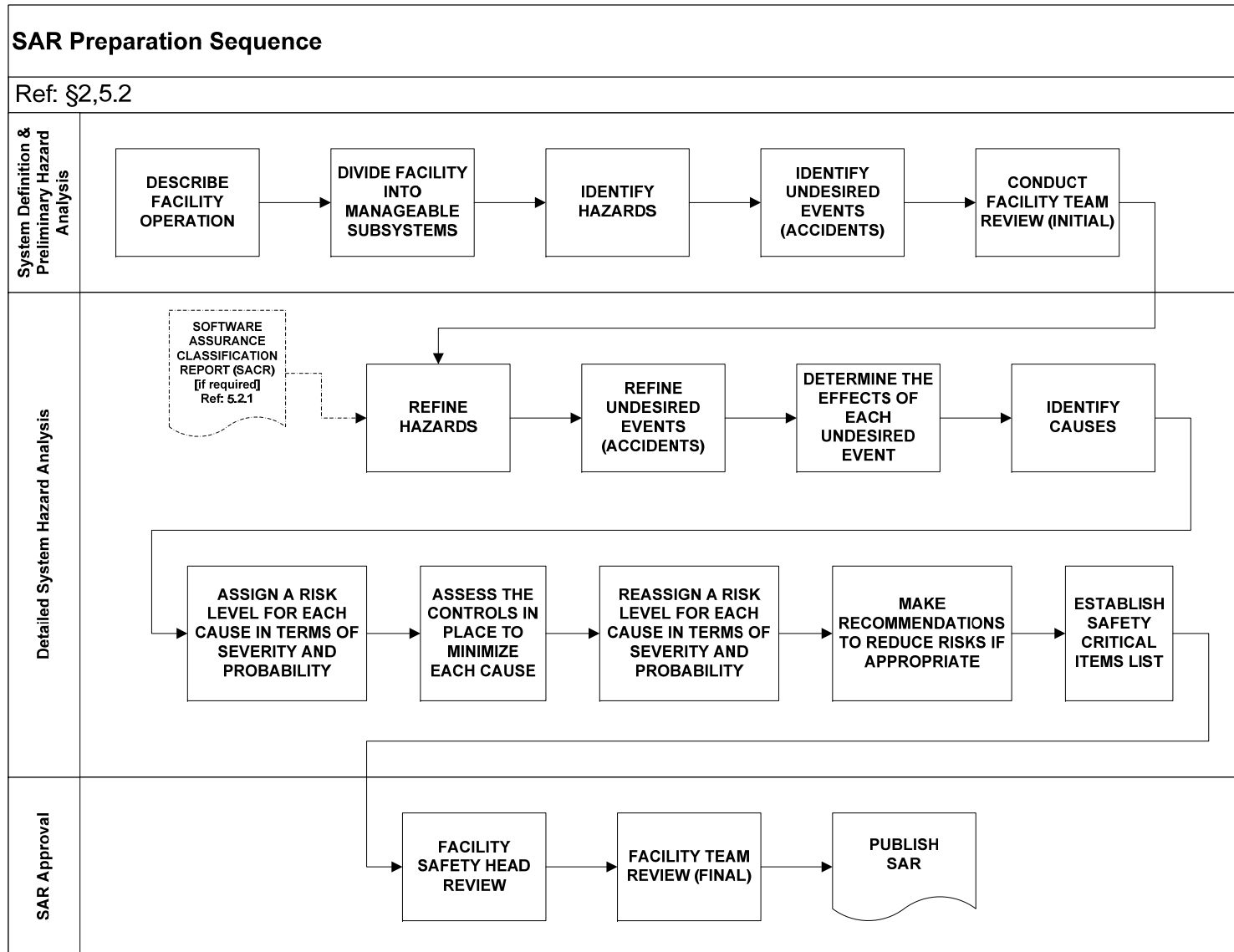


Figure 2-1 – SAR Preparation Sequence

- g. With the subsystems, Hazards, and Undesired Events defined, the FSSE prepares a Safety-Critical Items List.
  - 1) 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.
  - 2) The requirement for design calculations can be waived for safety-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.
  - 3) Safety-critical items listed in a SAR shall be tracked throughout their lifetime for compliance with design, maintenance, and inspection requirements.
  - 4) 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.
- h. At this point, a complete SAR is ready for a Facility Safety Head Review. The FSH conducts a thorough and independent review of the SAR.
- i. Once the FSSE and FSH agree that the SAR is complete, a Final Facility Team Review is conducted. During this phase, the remaining members of the Facility Team review the SAR.
- j. Finally, the SAR is published. After all of the issues are resolved and the SAR is prepared in final format, it shall be formally approved by the Safety Manager and FSH.
- k. Finally, it shall be incorporated into the CM Program.

#### 2.5.4.1.1 Hazard Analysis

- a. The HA begins with a detailed exploration of each of the identified hazards (e.g., hot surfaces).
- b. Considering that hazard, the FSSE 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/death, damage to the environment, or loss of productivity. When numerous effects result, only the most severe is noted.
- d. Next, the FSSE 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 2.5.4.
- g. To determine a facility's ability to avoid the occurrence of an undesired event, the FSSE 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 SFAB FSSE has assessed the current hazard controls, the RAC is re-evaluated using the guidance provided in Section 2.5.4.
- j. If an assigned RAC is unacceptable, as outlined in Section 2.5.4, 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.

#### 2.5.5 Risk Assessment

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

2.5.5.2 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, "Risk Assessment Matrix."

#### 2.5.5.3 Severity Category

2.5.5.3.1 A Severity Category shall be 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.

2.5.5.3.2 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.

#### 2.5.5.4 Probability of Occurrence Level

2.5.5.4.1 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.

2.5.5.4.2 The probability level shall be qualitatively based upon engineering judgment with appropriate guidelines. Those guidelines are Frequent, Occasional, Possible, and Remote.

**HAZARD SEVERITY**

Hazard Severity Categories provide a relative measure of the worst possible consequences resulting from personal 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**




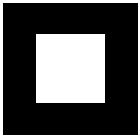


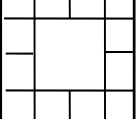

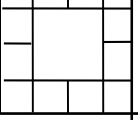
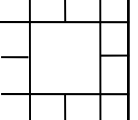
Hazard probability is the likelihood that a hazard will occur during the planned life expectancy of the system. The probability level is qualitative, based on engineering judgment, with appropriate guidelines as follows:

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

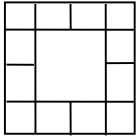
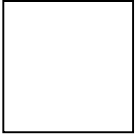
**LEVEL B - OCCASIONAL.** The level assigned when a safety feature does not exist, but the use of approved procedures should prevent the undesired event from occurring.

**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.

SEVERITY \ PROBABILITY	PROBABILITY				
	A FREQ	B OCC	C POSS	D REM	
I CATASTROPHIC					 RAC 1
II CRITICAL					
III MARGINAL					
IV NEGLIGIBLE					

	RAC 2
	RAC 3

**Figure 2-2 – Risk Assessment Matrix**

#### 2.5.5.4.3 Establishing a Risk Assessment Code

- a. First, the effect of an undesired event is evaluated in terms of Severity (I, II, III, or IV).
- b. Next, the probability of occurrence (A, B, C, or D) is determined for each cause of the undesired event. Using the severity of the undesired event, each cause is assigned its own unique alphanumeric risk level (e.g., IA, IIB, IIIC).
- c. Finally, using the two-dimensional risk matrix, Figure 2-2, each risk level is translated into one of three RACs - RAC 1, RAC 2, or RAC 3. They are pattern-coded on the matrix to distinguish each from the other. RAC 1s include blocks IA, IB, IC, IIA, IIB, and IIIA. RAC 2s include blocks IIC, IIIB, and IVA. All other blocks are RAC 3s. After the in place hazard controls are assessed, the above assessment is repeated using the newly established probability of occurrence.

#### 2.5.5.4.4 Implications of a Given RAC

- a. A **RAC** is a measure of the severity of an undesired event 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.
- b. **RAC 1s** are the most serious of the three 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 a RAC 1 shall be as listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility.
  - 1) **New/CoF Project** - RAC 1s for new facilities, and those associated with a Construction of Facilities (CoF) project in an existing facility, are of safety concern and require resolution (reduction of the RAC from 1 downward to 2 or 3) before the facility can initiate/resume operations.
  - 2) **Existing** - RAC 1s for existing facilities not undergoing a major CoF are a major safety concern and require one of the following before the facility can resume operations:
    - i. Resolution (i.e., reduction of the RAC from 1 to a 2 or 3), or
    - ii. An abatement plan approved by the Safety Manager, organizational director for the facility, organizational director for the employees 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 Risk Assessment. The implications of a RAC 2 shall be as listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility.
  - 1) **New/CoF Project** - RAC 2s for new facilities and those associated with a CoF 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, Safety Manager, organizational director of the facility, and the director of the employees within the facility have authorized operations to begin.

- 2) **Existing** - RAC 2s for existing facilities not undergoing a CoF require the approval of the director for the facility, director for the employees, and the Safety Manager before operations can resume. Plans and programs to correct existing RAC 2 UEs, 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, Safety Manager, and FSH. Acceptance of the risk associated with these undesired events is acknowledged by signing the SAR.

## 2.6 LARC INTERLOCK PHILOSOPHY

2.6.1 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 Interlock Philosophy, 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. Period of performance shall be established by the safety analysis and specified in the SAR.
- f. 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 in accordance with Chapter 3 and SCM in Section 5.2.2 of this procedure. 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 (temporary changes to complete a run or troubleshoot a problem) must 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.

2.6.2 The above philosophy shall 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.

#### 2.6.3 Design

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

#### 2.6.4. 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 the design features above, they are to be passive in nature and require no special action to cause them to be effective.

#### 2.6.5 Safety Devices / Personal Protective Equipment

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.

#### 2.6.6 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 undesired events. Warning devices are effective only when personnel are aware of them in sufficient time to react; and do, in fact, react.

## 2.6.7 Procedures/Training

2.6.7.1 The introduction of the human element into a perfectly 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 (ref: LPR 1740.7, "Process Systems Certification Program" for more details).

2.6.7.2 The process shall be controlled by SOPs. If operator training and procedure compliance are to be completely 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.

## 2.7 CRITERIA FOR DESIGNATING DOCUMENTS AND DRAWINGS AS CCDs

2.7.1 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 documents as CCD and placing these documents in the Facility CM Program. CCD will include the SAR, the SOPs and/or checklists, any pressure systems documents, and the key facility mechanical, weld, and electrical engineering drawings and schematics. The SFAB FSSE, FSH, and PM shall be responsible for designating a drawing as CCD. Any drawings:

- a. Supporting the conclusions of the safety analysis or
- b. Useful for troubleshooting systems (e.g., electrical, computer, mechanical) designated as CCD.

2.7.2 Members of the Facility Team may include other documents and drawings as CCD, if desired.

2.7.3 The Safety Manager shall have the responsibility for resolving any differences of opinion and making final decisions regarding the disposition of all documents and drawings chosen for inclusion in the CM Program.

## CHAPTER 3.0 – FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM

### 3.1 PROGRAM SUMMARY

3.1.1 The LaRC Facility CM Program includes FRI-1 facilities listed in 00-MSC-ECSUM, Effort Code Summary provides for the ability to:

- a. Record and maintain safety analysis documentation,
- b. Document and maintain SOPs for use by operating personnel,
- c. Ensure the SFAB reviews changes that affect safety, and
- d. Establish and maintain a baseline for designated systems (e.g., electrical systems, mechanical systems, computer systems) and the relevant configuration control documentation (e.g., drawings).

*Note: The facility's computer system baseline shall be established and maintained per the Software CM and Computer System Inventory programs; reference sections 5.2.2, Software Configuration Management, and 5.2.3, Computer System Inventory.*

3.1.2 In addition, the Facility CM Program provides for risk reviews that consist of Procedure Demonstrations and continual Facility System Safety Engineering Analyses.

### 3.2 CHANGE CONTROL

3.2.1 The cornerstone of LaRC's Facility CM Program is the Change Notification Sheet (CNS) process. Any change to facility hardware that affects safety, CCD drawings, a SAR and/or SOPs shall be processed through the CNS process.

3.2.2 Changes to pressure systems documents (PSD) shall also be processed using the CNS process. This process ensures notification of the change to the affected parties, verification that no protective measures have been degraded or defeated, and that no new hazards have been introduced.

3.2.3 The CNS process requires the FC, the FSH, the FCC, and the Safety Manager or designee to approve a CNS prior to any hardware changes.

3.2.4 A safety and/or third party review shall be conducted for all modifications except those that are strictly administrative in nature. All affected documents (e.g., SARs, SACRs, SOPs, checklists, drawings) are redlined prior to implementation of the change.

3.2.5 The CNS process shall be conducted in accordance with one of two LMS Center Procedures (CPs) – LMS-CP-4710, "Configuration Management for Facilities" and LMS-CP-4890, "Construction and Change Assurance for High-Risk Facilities."

3.2.6 LMS-CP-4710 shall be used for minor changes, such as replacing a high-pressure valve with an equivalent component or a change that does not affect safety. More complex changes, such as adding a new system or a change that impacts safety shall be conducted in accordance with LMS-CP-4890. Additional information to determine which LMS process shall be used is provided in Section 3.4, "Types of Change".

3.2.7 SOPs/checklists that have had redlines approved by the FSH shall be submitted to the CNS process within thirty (30) days of approval.

### **3.3 UPDATING AND DISTRIBUTING CCDS**

- a. All CCDs shall be updated in accordance with the redlined documents submitted through an approved CNS. Updating CCDs shall not occur until after the changes proposed by the CNS have been completed. All updated CCDs shall be distributed as outlined in this section.
- b. For each CNS completed, a notice shall be sent to the FSH and FC that includes at least the following information: CNS Number and Description of Change. The facility shall receive a package that includes the "Working Master(s)".

### **3.4 TYPES OF CHANGE**

- a. Modifications to facilities at LaRC under the CM Program can be one of four types:
  - 1) Administrative change,
  - 2) No safety impact,
  - 3) Safety impact and construction not required, and
  - 4) Safety impact and construction required.
- b. The CNS process depends upon which of these four types of changes is occurring. The four methods are discussed in the paragraphs that follow.

#### **3.4.1 Administrative Change**

3.4.1.1 Facility modifications that are simply administrative in nature and do not affect safety can be implemented without a CNS. An example of such changes is the replacement of a mechanical or electrical component with an equivalent component or a typographical error in a SOP/checklist or SAR.

3.4.1.2 A CNS shall be required to update Pressure Systems Documents (PSDs) when like-for-like replacements are made in a high-pressure system, and

3.4.1.3 The CNS process shall be conducted in accordance with LMS-CP-4710.

### 3.4.2 No Safety Impact

Changes that require updating CCD but are initiated as no safety impact shall be processed in accordance with LMS-CP-4710. Even though the CNS has been marked “safety not affected,” LMS-CP-4710 requires a safety review to ensure no safety impact exists.

### 3.4.3 Safety Impact

3.4.3.1 For those facility modifications that affect safety, the CNS process shall be conducted in accordance with LMS-CP-4890. The primary objective of this process is to ensure the appropriate safety analysis is conducted and that existing CCD documents are updated and, if required, new CCD documents are identified.

3.4.3.2 There are two possible “paths” through this process. The path chosen depends on whether the change is being conducted in accordance with LAPD 7000.2, “Review Program for Langley Research Center (LaRC) Facility Projects.” Changes governed by LAPD 7000.2 are conducted as outlined in Section 3.4.4, “Change Controlled by Design Review Process.”

3.4.3.3 For changes not governed by LAPD 7000.2, a CNS shall be initiated and submitted through the CMOL system.

3.4.3.4 Affected redlined CCD documents supporting the change shall be appended to the CNS and the electronic package forwarded through the FSH to the Safety Manager, or designee.

3.4.3.5 Prior to the Safety Manager's approval, the SFAB FSSE responsible for the facility shall conduct a safety analysis.

3.4.3.6 After approval by the Safety Manager or designee, the package shall be forwarded to the FCC for approval.

3.4.3.7 When the change is completed, the final redlined “as-built” documents and field-verified drawings shall be submitted via the CNS for document/drawing update.

### 3.4.4 Change Controlled by Design Review Process

3.4.4.1 This method is used for major modifications that are governed by LAPD 7000.2, “Review Program for Langley Research Center (LaRC) Facility Projects.” For changes in this category, the information below pertains:

- a. Prior to the Preliminary Design Review (PDR), the PM, in coordination with the FSH and FC, shall ensure that the affected portions of all existing drawings, including interface drawings, impacted by the project are field verified (FV) and redlined to reflect the true configuration of the facility.

- b. At the PDR, the SFAB FSSE shall report on the FV status of the above mentioned drawings and present the results of the safety analysis.
- c. Prior to the Critical Design Review (CDR), all existing and proposed CCD documents shall be redlined to accurately reflect the intended configuration of the facility. Also, the PM shall have a Field Verification Plan to ensure all CCD drawings are field verified prior to the Integrated System Review (ISR).
- d. At the ISR, the FSSE shall attest that all drawings previously identified as CCDs have been FV and present the results of the safety analysis.
- e. Following the ISR, the PM shall initiate a CNS that covers the project. This CNS shall identify all existing CCD drawings, or other documents, and any new drawings/documents that are to be CCDs.
- f. At the ORR, the FSSE shall provide the final, approved redlined SAR. The PM shall also provide a complete set of “as-built” redlined drawings signed off and approved as FV.
- g. At the completion of the ORR, the above-mentioned redlined documents shall be forwarded via the CNS for incorporation into the CM Program

### **3.5 CONFIGURATION CONTROL DOCUMENTATION – DRAWINGS**

This section describes several unique aspects of drawings incorporated into the CM Program and designated as CCD. Section 2.7, “Criteria for Designating Drawings as CCDs” provides guidelines for which drawings shall be placed under configuration control.

#### **3.5.1 Drawing Field Verification**

3.5.1.1 All engineering drawings currently in the CM Program shall be classified as either FV or unverified.

3.5.1.2 Additionally, no new drawing shall be brought into the CM program (i.e., designated as CCD) unless it is first FV.

3.5.1.3 The field verification process shall be a hands-on verification of the validity of the drawing conducted by facility, SFAB, PEB, or contractor personnel.

3.5.1.4 A drawing which has been FV shall display a "FIELD VERIFIED" statement authenticating that action.

3.5.1.5 That statement shall be signed by the person attesting to the field verification.

3.5.1.6 It shall also be signed and dated as approved by the PM, FSH, or FC.

3.5.1.7 If FV drawings are found to be discrepant, they shall lose their FV status and shall be identified as unverified. A sample of the FV statement is as shown below:

<p><b>FACILITY BASELINE DRAWING</b></p> <p><b>FIELD VERIFIED BY:</b> _____</p> <p><b>APPROVED BY:</b> _____</p> <p><b>LATEST DATE:</b> _____</p>
--

3.5.1.8 Drawings that are in the CM Program but are not FV shall display a "WARNING! UNVERIFIED" statement alerting the user that they are not field-verified. A sample of that warning label is as shown below:



3.5.1.9 All drawings that are currently in the CM Program and not FV are subject to an ongoing field verification effort by facility and PEB personnel as time and resources permit.

### 3.5.2 Changes to CCD Drawings

3.5.2.1 When drawings in the CM Program require change, the drawing shall be redlined. Drawings may be redlined manually or electronically.

3.5.2.2 Drawings that are redlined manually shall be redlined as follows:

- a. New items shall be added in green ink or black ink highlighted in yellow marker.
- b. Existing items requiring deletion shall be marked out with red ink.

3.5.2.3 Drawings that are redlined electronically shall be redlined as follows:

- a. All items being changed (added/deleted) shall be outlined in a cloud format.

- b. New items shall be added in green.
- c. Existing items requiring deletion shall be marked out with red.

3.5.2.4 Redlined drawings shall be processed using the CNS process.

3.5.2.5 The new original drawings shall be delivered to Engineering Drawing Files (EDF) and new WORKING MASTER copies delivered to the facility.

### 3.5.3 Working Masters

3.5.3.1 For each CCD drawing, the facility shall be provided a current revision of the drawing marked "WORKING MASTER" in red ink. The intent of this procedure is to identify the drawing as a copy of the current configuration of the facility as described by the Master (reproducible) drawing.

3.5.3.2 These WORKING MASTER drawings shall be kept in a central location at the facility and closely controlled to ensure availability to facility personnel.

3.5.3.3 In those cases where there are a number of CCD drawings with detail systems that affect more than one facility, each of the affected facilities will be listed, by EC, on the CCD sticker applied to the drawings.

3.5.3.4 In addition, each of the affected facilities shall receive a new drawing marked WORKING MASTER in red ink.

3.5.3.5 In this manner, each facility shall maintain a complete file of WORKING MASTER drawings that reflect the current configuration. With multiple copies of a WORKING MASTER, the situation can exist where one facility may have modified a system, including the redlining of the affected drawings, without informing the other facility having a WORKING MASTER of the same drawing.

3.5.3.6 To preclude any adverse impact of changing a drawing with multiple ECs, the FSH shall ensure that a CNS has been approved before modifying their facility.

3.5.3.7 Adherence to the following additional guidelines promotes accountability and use of WORKING MASTER drawings:

- a. A WORKING MASTER drawing shall always reflect the true ("as-built") configuration of the facility it represents.
- b. Proposed changes to a facility which impact a CCD drawing shall be redlined on a separate copy of the affected drawing, not on the WORKING MASTER.
- c. Changes, which reflect "as-built" configurations, shall be marked on the WORKING MASTER of each affected CCD drawing.
- d. The current WORKING MASTER (or a copy of it) shall always be present at the facility.



### **3.6 FACILITY BASELINE LIST (FBL) AND SUPPORTING FACILITY DOCUMENTS**

3.6.1 An FBL can be generated for each facility in the CM Program using CMOL.

3.6.2 The FBL represents a list of all CCD documents for the Facility. For those facilities that choose, a list of Supporting Facility Documents (SFDs) will be maintained on CMOL.

3.6.3 SFDs are documents/drawings that are affiliated with the facility but not under CM control. It shall be the responsibility of the FSH or FC to update the list of SFD and submit any changes to CMOL. SFDs are not CCDs, and their configuration is not maintained as part of the CM Program. Revision of SFD drawings is the responsibility of the facility since they are not CCD.

### **3.7 FILING SYSTEMS FOR CCDS**

The documents in the CM Program are stored as described in the following paragraphs.

#### **3.7.1 EDF**

3.7.1.1 EDF shall be the repository for all original (reproducible) configuration controlled drawings and for the electronic historical records of configuration controlled drawings and other CCDs. EDF will preserve these historical records and all subsequent changes.

3.7.1.2 Only a CM Representative, with the CM contractor maintaining CMOL, shall be permitted to withdraw CCD original drawings from EDF.

3.7.1.3 Analyses, drawings, and nondestructive engineering information for systems that have been recertified or identified as safety-critical shall also be stored in EDF.

#### **3.7.2 Facility Files**

3.7.2.1 Each facility shall maintain its own filing system of current WORKING MASTER CCDs.

3.7.2.2 Facilities must ensure that updates to WORKING MASTERS are posted and centrally stored so as to be of use when needed.

### **3.8 RISK AND SAFETY REVIEW**

The risk and safety review aspect of the CM Program consists of Annual Safety Meetings, Procedure Demonstrations, and continual Facility System Safety Engineering Analyses.

### 3.8.1 Annual Safety Meetings

3.8.1.1 Annual Safety Meetings are held for each LaRC facility. Facilities under the CM Program. The meetings shall have an additional agenda item added for the review of facility documents, status, plans, and CM program effectiveness. These meetings are scheduled by an SFAB Representative.

3.8.1.2 The SFAB Representative shall issue a letter summarizing the meeting and delineating "action items." Facilities shall maintain a copy of the meeting letter in the Facility Resume.

### 3.8.2 Procedure Demonstrations

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

- a. FSH
- b. CM Representative
- c. Certified Operator(s)
- d. SFAB Representative

3.8.2.2 Procedures that have not been verified or used within the last 12 months shall be verified by a Procedure Demonstration.

3.8.2.3 At the completion of a Procedure Demonstration, the CM Representative shall notify all participants which procedures were demonstrated.

3.8.2.4 The FSH shall ensure any changes required based on the procedure demonstration are submitted via CNS.

### 3.8.3 Continual Facility System Safety Engineering Analyses

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

## 3.9 CONFIGURATION MANAGEMENT ON-LINE

CCDs in the LaRC Facility System Safety Program are accessible electronically and the CNS process is implemented electronically. The CMOL system provides for searching and viewing CCDs and provides for electronic CNS processing (i.e., CNS Workflow).

### 3.9.1 Access and Database Maintenance

- a. Access to CMOL shall be by authorized personnel at <https://cmol.ndc.nasa.gov/>.
- b. Entry into the CMOL system shall be controlled by use of an employee's Agency User ID (AUID) and associated password.
- c. SFAB shall approve any request for an account that requires authority to approve a CNS.
- d. New documents shall be entered into the CMOL database within 10 working days of final approval. If there is a question concerning the currency of a particular document, contact a representative from SFAB for assistance and/or confirmation.

### 3.9.2 CNS Initiation/Processing

3.9.2.1 At the CMOL homepage, the user selects the "LF 127, Change Notification Sheet (CNS) Workflow System" to initiate, approve, or view a CNS. The CNS workflow screen displays three options from which to select.

3.9.2.2 The first option allows the user to create a new CNS Work Package on line, and the second allows for searching for a particular CNS Work Package that is already in the system.

3.9.2.3 The third option allows the user to view the status of CNS Work Packages over which the user has authority or that require the user's attention (i.e., review and approval).

## CHAPTER 4.0 – PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM)

### 4.1 PROGRAM SUMMARY

4.1.1 As part of LaRC's Pressure Systems Recertification Program, a PSD is developed for ground-based high-pressure systems. For additional information about the Pressure Systems Recertification Program, refer to LPR 1710.42, "Safety Program for Recertification and Maintenance of Ground-Based Pressure Vessels and Piping Systems." The Pressure Systems Configuration Management (PSCM) Program maintains the configuration control of all PSDs using the CNS process outlined in Chapter 3 of this document.

4.1.2 Any change, whether administrative in nature or not, to a high-pressure system covered by LaRC's Recertification Program shall be documented using the CNS process.

4.1.3 Changes that are administrative in nature, such as replacing a high-pressure valve with an equivalent component, shall be performed in accordance with LMS-CP-4710, "Configuration Management for Facilities."

4.1.4 Other changes shall be conducted in accordance with LMS-CP-4890, "Construction and Change Assurance for High Risk Facilities".

4.1.5 After a change has been approved and the work has been completed, all affected documentation shall be field verified and updated in CMOL.

Any discrepancies found during the field verification shall be appropriately redlined and reviewed by the Standard Practice Engineer (SPE) for Pressure Systems and the FSH prior to incorporation into the CCD.

### 4.2 PRESSURE SYSTEMS DOCUMENT

4.2.1 The SPE for Pressure Systems shall ensure that PSDs are produced for all ground-based high-pressure vessels/systems in accordance with LPR 1710.42, "Safety Program for Recertification and Maintenance of Ground-Based Pressure Vessels and Piping Systems." The PSD is a compendium of component information and sketches and consists of:

- a. **Title Page** – Identifies the document as a PSD, the facility number and name, the system name and designation, and the PSCM document number
- b. **PSCM Revision Record** – Reflects the approval of all issues of the PSCM
- c. **Table of Contents**
- d. **Introduction** – Discusses the development, purpose, and uses of PSCM
- e. **Definition of Symbols**
- f. **Key to Recertification Sheets** (Component Inventories)
- g. **System Description**
- h. **Isometric Drawings**
- i. **Recertification Status Sheets**
- j. **Footnotes**
- k. **Document Reference Sheet**

## **CHAPTER 5.0 – FACILITY SOFTWARE ASSURANCE AND SOFTWARE CONFIGURATION MANAGEMENT**

### **5.1 GENERAL**

5.1.1 The use of automated control systems, programmable logic controllers (PLC), standalone controllers and other supported software systems by LaRC research facilities has established the need for configuration control of software.

5.1.2 This chapter outlines the requirements for the SCM, Software Assurance Classification, and Computer Inventory programs at LaRC research facilities.

5.1.3 This chapter applies to software that resides in hardware (i.e., firmware) and safety-critical software including Data Acquisition System (DAS) and computer systems used in the automation of electromechanical processes (e.g., PLCs).

5.1.4 The requirements as specified in Chapter 5, Facility Software Assurance and Configuration Management, are required for all FRI 1 (High Risk) utilizing safety-critical software.

5.1.5 The requirements as specified in Chapter 5 are recommended for all other facilities.

### **5.2 PROGRAM OVERVIEW**

#### **5.2.1 Software Assurance Classification**

5.2.1.1 Each research facility using an automated control system that is responsible for performing safety-critical functions shall develop a SACR. The report identifies software safety-critical functions prior to and during implementation.

5.2.1.2 The SACR shall be developed in accordance with NASA-STD-8719.13B and placed under configuration control in CMOL.

5.2.1.3 For a facility developed prior to the first release of NASA-STD-8719.13B, a new SACR that meets the requirements of NASA-STD-8719.13B is not required until new software is developed/acquired; however, if the existing SACR does not clearly define a process to classify safety-critical systems, a new SACR shall be developed.

#### **5.2.2 SACR Preparation**

5.2.2.1 The Safety Manager shall appoint a SFAB FSWSE to be responsible for the preparation of a SACR. The actual preparation is performed by the SFAB/SMAO FSWSE or a FSWSE from a support contractor.

5.2.2.2 FSE shall support this effort on an as-required basis.

5.2.2.3 Any SACR prepared by a support contractor shall be reviewed and approved by the SFAB/SMAO FSWSE.

5.2.2.4 The approach taken is reflected in Figure 5-1, "SACR Preparation Sequence."

### 5.2.3 SACR Phases

5.2.3.1 Describe computer systems operation, identify computer systems and subsystems, compile inventory of computer systems (reference 5.2.3 Computer System Inventory), evaluate computer systems to determine their safety criticality, and identify software risk mitigations and software hazard causations.

5.2.3.2 Determine software safety criticality using the criteria as specified in the *NASA Software Safety Standard* and complete Software Safety Litmus Test (reference NASA-STD-8719.13B §4.1.1.2).

5.2.3.3 At this point, a complete SACR is ready for an FSH Review. The SFAB/SMAO FSWSE conducts a thorough and independent review of the SACR.

5.2.3.4 Once the SFAB/SMAO FSWSE agrees that the SACR is complete, a Final Facility Team Review is conducted. During this phase, the remaining members of the Facility Team review the SACR.

5.2.3.5 Finally, the SACR is published. After all of the issues are resolved and the SACR is prepared in final format, it shall be formally approved by the Reliability and Quality Assurance, Safety Officer, and FSH. Finally, it shall be incorporated into the CM Program.

### 5.2.4 SACR Organization

5.2.4.1 The SACR is divided into sections; Introduction, Project Background/Function Description, Reference Documents, Software Classification, Software Safety Litmus Test, Software Assurance Effort, and Appendices.

5.2.4.2 The SACR can be further subdivided into subsections such as Hazard Analysis and Software Configuration Management common to all facilities although, on a case-by-case basis, additional special-item subsections (e.g., Computer System Inventory List) can be added.

### 5.2.4 SACR Changes and Distribution

5.2.5.1 The SACR is reviewed and updated on an as-needed basis as in the case when an electromechanical device is replaced with a PLC.

Since SACRs are CCDs, they shall be changed and distributed in accordance with the requirements set forth in Chapter 3 of this document.

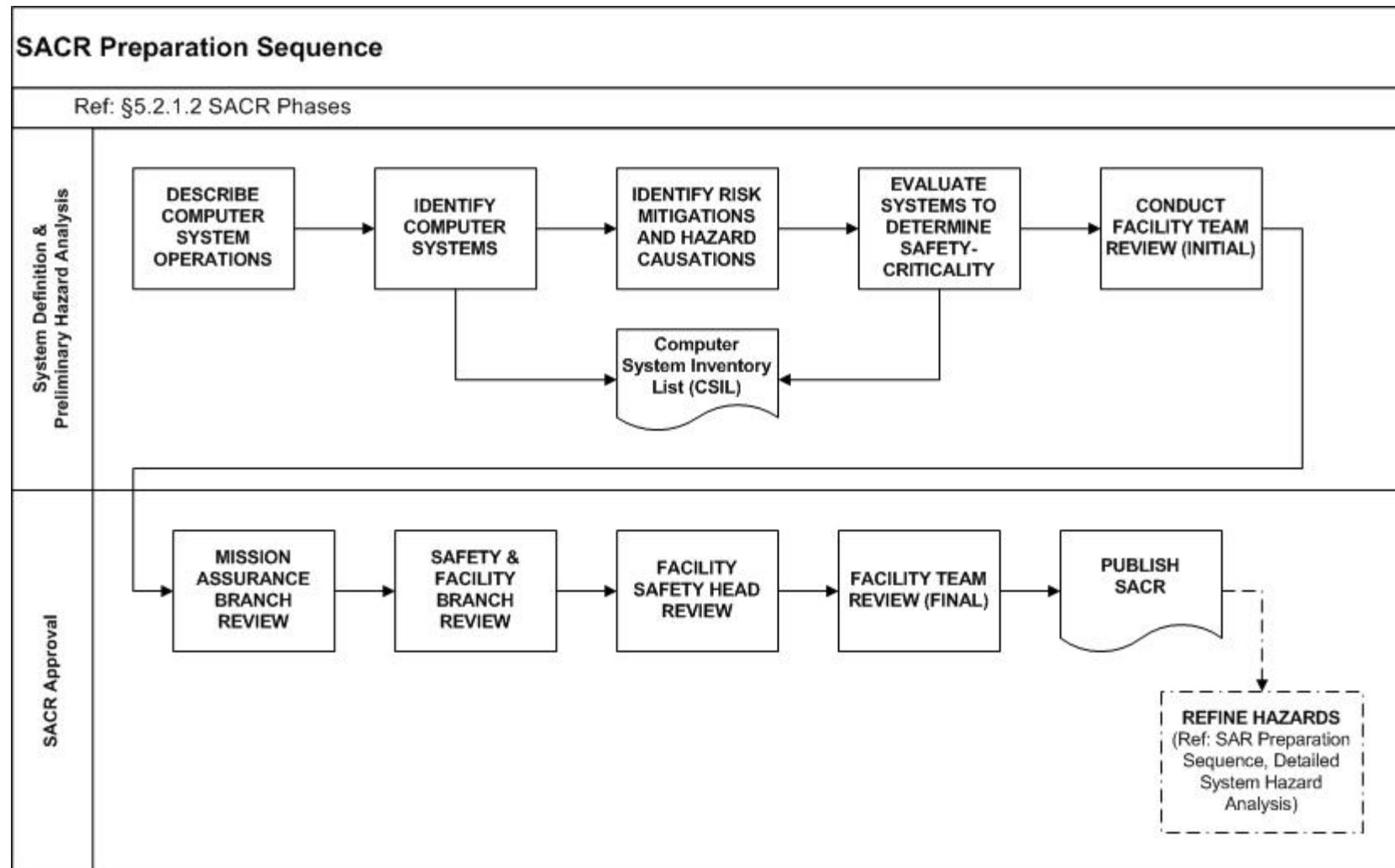


Figure 5-1 – SACR Preparation Sequence

## 5.2.5 Software Configuration Management

5.2.6.1 The configuration control of software products is performed per a Software Configuration Management Plan (SCMP) when a facility employs a system that includes software that performs safety functions (e.g., correct valve sequencing, shutdown the facility in an overtemperature condition). The SCMP may be facility-specific or may be general with facility-specific elements.

5.2.6.2 Each research facility using an automated control system that is responsible for performing safety-critical functions (e.g., correct valve sequencing, shutdown the facility in an overtemperature condition) shall develop a SCMP.

5.2.6.3 The SCMP shall define a process to identify and review changes that directly affect safety-critical software prior to implementation and during operation and maintenance.

5.2.6.4 All changes, modifications, and patches made to safety-critical requirements, design, code, systems, equipment, test plans, procedures, simulators, models, test suites, or criteria shall be evaluated.

5.2.6.5 All changes to baselined safety-critical software shall be approved.

5.2.6.6 The required level of configuration control during development shall meet the requirements of LMS-CP-5529, "Software Configuration Management Planning for Low, High-, and Critical-Control Software."

5.2.6.7 The SCMP shall be developed in accordance with LMS-CP-5529.

5.2.6.8 Commencing at the ORR, software changes that might affect facility safety and/or a SAR Undesired Event hazard control (e.g., interlocks, valve sequencing) shall be subjected to a review by the FSH, the FC, a SFAB FSSE/FSWSE, and a PEB representative.

5.2.6.9 Additional measures may be taken to identify and review changes that directly affect safety prior to implementation, such as:

- a. Evaluate hazards for software's contribution (cause, control, etc.)
- b. Conduct software safety analyses; coordinate with the system safety analyses
- c. Create software safety requirements
- d. Analyze and report software safety non-conformances to appropriate personnel
- e. Review system hazard analyses for changes that impact the software subsystem
- f. Inform system safety personnel of changes in safety-critical software



5.2.6.10 The SCMP shall be placed under configuration control. There are two possible “paths” through this process:

a. CMOL

(1) The SCMP shall be placed under configuration control in CMOL.

b. Virtual Library

(1) The SCMP shall be placed under configuration control in ROME Virtual Library.

(2) A copy of the SCMP shall be placed under configuration control in CMOL.

(3) Alternatively, a placeholder shall be placed under configuration control in CMOL with a reference to the SCMP under configuration control in ROME Virtual Library.

(4) Regardless of path, all provisions of Chapter 5 shall apply.

5.2.6.11 The CNS process shall be used to track and control software changes whenever they might affect facility safety and/or a SAR Undesired Event hazard control. The CNS also ensures that other CCD documents (e.g., SAR, SACR) are updated as required. The Facility Software Configuration Manager (FSCM) shall initiate the CNS.

5.2.6.12 If the FSCM has any question about the safety impact of a change, the FSH, a FSE, or a SFAB FSSE/FSWSE shall be consulted.

5.2.6.13 The FSCM shall be identified in the SCMP.

5.2.6.14 For a facility with a SCMP developed prior to the first release of LMS-CP-5529, a new SCMP that meets the requirements of LMS-CP-5529 is not required until new software is developed/acquired.

5.2.6.15 A new SCMP shall be developed if the existing SCMP does not clearly define a process to review changes that impact safety.

5.2.6.16 The SCMP is reviewed and updated on an as-needed basis (e.g., changes to NASA or Center processes or procedures for managing safety-critical software, new software is developed and/or acquired).

## 5.2.6 SCMP Preparation

5.2.7.1 The Facility Safety Head shall appoint a FSCM to be responsible for the preparation and maintenance of the SCMP. The actual preparation may be performed by either the FSE or a FSE from a support contractor.

5.2.7.2 Any SCMP shall be reviewed and approved by the SFAB FSWSE.

## 5.2.7 Computer System Inventory

5.2.8.1 Each research facility utilizing safety-critical software systems, a Computer System Inventory List (CSIL) shall be maintained.

5.2.8.2 The CSIL shall contain an inventory of software that resides in hardware (i.e., firmware) and safety-critical software, including DAS and computer systems used in the automation of electromechanical processes (e.g., PLCs).

*Note: How computer systems and software systems (e.g., software applications) are identified in any given facility will depend on a number factors including the software development methodology(ies) used. Especially for computer systems, each facility might have very unique naming and identification conventions. Whatever identification schema is used; it should facilitate the tracing of safety-critical software between the SACR and the SAR.*

5.2.8.3 For each computer system listed in the CSIL, the computer identifier, the computer model, the configuration control documentation (e.g., drawings), and the software systems (e.g., the application software) shall be identified.

5.2.8.4 Although the CSIL can be a standalone document, the required information can be incorporated in other documents (e.g., SACR) or applications (e.g., information captured into the ROME Virtual Library). If not included in the SACR, the SACR shall identify where the inventory is maintained.

*Note: If the required CSIL information is not maintained under CMOL control. It shall be maintained in an appropriate and controlled environment (e.g., ROME Virtual Library).*

5.2.8.5 The CSIL shall be reviewed annually and updated as needed (e.g., new software is developed and/or acquired).

## 5.2.8 CSIL Preparation

5.2.9.1 The Facility Safety Head shall appoint a Facility Systems Engineer to be responsible for the preparation and maintenance of the CSIL. The actual preparation is performed by either the FSE or a FSE from a support contractor.

5.2.9.2 Any CSIL shall be reviewed by the SFAB FSWSE.

## CHAPTER 6.0 – LANGLEY RISK EVALUATION PROGRAM

### 6.1 PROGRAM SUMMARY

6.1.1 The LREP has been established to provide a systematic review of the energy sources utilized by research equipment and operations at LaRC that are not in the CM Program and not covered with a Safety Permit. This review mechanism allows SFAB to identify any potential hazards associated with these energy sources and identify the proper controls for the energy sources. As shown in Figure 6-1, equipment/operations using energy sources at or above the identified levels that are not in the CM Program and not covered by a Safety Permit shall be reviewed by SFAB for inclusion into LREP before the equipment is purchased and installed on Center.

Equipment/Operations Required for Review		
<b>Electrical</b> <ul style="list-style-type: none"> <li>Permanently installed, operating at or above 50 VAC/VDC.</li> </ul> <u>Example:</u> Wind-tunnel motor, 240-volt, 3-Phase.	<b>Thermal</b> <ul style="list-style-type: none"> <li>External surfaces in excess of 130°F.</li> <li>Internal temperatures in excess of 212°F.</li> <li>Utilizing cryogenic fluids.</li> </ul> <u>Example:</u> Vacuum Furnace, Operates internally to 3000°F	<b>Pressure</b> <ul style="list-style-type: none"> <li>All pressurized/vacuum systems.</li> </ul> <u>Example:</u> MTS test stand, hydraulic pressure at 3000psi
<b>Human Interactions</b> <ul style="list-style-type: none"> <li>Requires the use of an external piece of equipment (e.g., laptop, pendant) to operate.</li> </ul> <u>Example:</u> MTS test stand with personal computer workstation provides main user-interface.	<b>Chemical Reactions</b> <ul style="list-style-type: none"> <li>Utilized to initiate chemical reactions or a byproduct of operations.</li> </ul> <u>Example:</u> Plasma flow control apparatus generates ozone and other pollutants as a byproduct.	

**Figure 6-1 – Equipment/Operations LREP Energy Source Levels**

6.1.2 Facilities that are not in the CM Program and not covered with a Safety Permit and have been identified with an FRI of 2 shall be included in the LREP program, (see Appendix C.2.2 for more information) and any other system that has been determined by SFAB to be included in LREP.

6.1.3 Equipment/Operations held under the former Laboratory Risk Evaluation Program are excluded from the requirements of this Chapter until an update is required. At that time, the equipment/operations shall be evaluated under this Chapter.

6.1.4 The elements associated with the LREP program are an LRE and a Langley Operating Procedure. These documents shall be maintained in the Facility Resume.

## 6.2 LANGLEY RISK EVALUATIONS

6.2.1 The term LRE was established to identify the Safety Analysis efforts associated with the LREP. An LRE documents the hazard analysis performed on equipment installed on Langley property. In most cases, the analysis is based on data from manufacturers' handbooks, discussions with certified operator and maintenance personnel, visual inspections, maintenance factors, and procedures. Management personnel shall take the steps necessary to implement any recommendations identified in the LRE.

6.2.2 An LRE consists of a Title Page, Revision Record, and a series of tables: Identification of Equipment, Energy Source(s), Hazard Controls, Identified Langley Operating Procedures (LOPs), and General Observations/Recommendations. Each section is described in further detail below:

- a. **Title Page** – Identifies the document as an LREP product, states the name of the equipment, and provides the number of the facility where the equipment is located.
- b. **LREP Revision Record** – Reflects the approval signatures for the initial issue and all LRE changes.
- c. **Identification of Equipment** – Gives the name of the equipment, purpose or nature of research/operation that can be conducted with the equipment, installation date, and the number of certified operators required to utilize the equipment.
- d. **Energy Source(s)** – All the energy sources associated with the operation of the equipment are identified (e.g., for Electrical, state the voltage and amps used by the equipment; for Pressure, state the medium and pressure).
- e. **Energy Controls** – Provides for the identification and location of all controls that will isolate the energy from the equipment and bring the equipment into a dormant state.
- f. **LOPs** – Identifies the associated LOPs, which have been developed in accordance with Appendix D of this LPR and are utilized by certified operators while operating the equipment
- g. **General Observations/Recommendations** – Provides an assessment of the equipment's operational environment to address any existing conditions that may be impacted by the new/changed equipment. Also, investigates the new/changed equipment effects on the facility and nearby operations (e.g., noise levels, power demands, effects of equipment malfunction). Establishes recommendations, if any identified new/existing conditions present unacceptable risk to personnel or equipment.

## 6.3 LANGLEY OPERATING PROCEDURES

6.3.1 LOPs shall be developed in accordance with Section 2.4 of this LPR with the following exceptions:

- a. Unique identifying number for LOPs shall be derived simply by adding a "P" to the identifying number of the LRE the procedures support (e.g., 1148-IP, 1148-2P).

## **6.4 LRE AND LOP CHANGES AND DISTRIBUTION**

6.4.1 LREs and LOPs shall be reviewed during the annual Facility Resume review by the FSH.

6.4.2 If the review determines that changes are necessary to the LRE and/or LOP, the following actions shall be completed:

- a. FSH shall redline the LRE and/or LOP and submit the requested change to their assigned SFAB FSSE
- b. SFAB FSSE shall review/approve the proposed redlined LRE and/or LOP
- c. SFAB FSSE shall revise the original LRE and/or LOP based upon the approved red-lined documents.
- d. After the LRE and/or LOP has been revised, the SFAB FSSE shall forward the LRE and/or LOP to the FSH for review/approval.
- e. The original revised LRE and/or LOP shall be entered in CMOL by SFAB.
- f. A working copy of the revised LRE and/or LOP placed into the facility resume and reviewed annually.

## APPENDIX A. DEFINITIONS

**Cause** – The stimulus or triggering mechanism/act that precipitates an Undesired Event Accident.

**Change Notification Sheet (CNS)** – NASA Langley Form 127, “Change Notification Sheet,” prepared by LaRC personnel and processed by contractor personnel. The CNS action is processed electronically via the LaRC Configuration Management On-Line (CMOL) system. It is used in the LaRC Facility System Safety Program to request approval of and record all changes in the affected facility and to its supporting CCDs.

**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 CM Program.

**Computer System** – A group of hardware components and associated software designed and assembled to perform a specific function or group of functions.

**Computer System Inventory List (CSIL)** – A CSIL is a listing of Computer Systems for the affected facility.

**Configuration Controlled Document (CCD)** – Facility baseline document 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, CCDs are revised only through a formal change process under the CM Program. Examples of CCDs 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)** – A discipline that establishes a baseline for facilities, selects technical and administrative documents, and exercises administrative control of all approved changes to that baseline.

**Configuration Management On-Line (CMOL)** – A web-based server which enables users to access LaRC facility CCDs electronically via their desktop computer.

**Configuration Management (CM) Representative** – Personnel supporting the LaRC Facility CM Program.

**CM Update** – The process of reviewing and documenting changes on a continuing basis. During this process, the reproducible masters (originals) of the affected documents are revised to incorporate the changes as shown on redlined documents. Revisions are initiated and tracked by the use of the CNS Form.

**Effect** – The consequence of an undesired event/accident 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 Facility CM Program. For the life of the facility, all CCDs will bear this number regardless of any facility name changes and/or hardware modifications.

**Facility Baseline List (FBL)** – A list of all CCD documents that can be generated using CMOL.

**Facility Configuration Coordinator (FCC)** – An individual appointed from the Project and Engineering Branch (PEB) who coordinates the support to the LaRC Facility System Safety Program. The FCC is also one of the approving officials for CNSs prior to any CM facility hardware changes that affect CCD documentation.

**Facility Coordinator (FC)** – An individual appointed to coordinate the overall day-to-day operations of a LaRC facility. This individual uses assigned facility personnel, and additional support personnel as available, to accomplish the FC requirements listed in this handbook.

**Facility Manager (FM)** – An individual who ensures safe and efficient utilization of the facility in support of research programs internal and external to NASA.

**Facility Risk Indicator (FRI)** – An initial safety assessment used to help determine the level of system safety effort required for a facility to meet NASA-LaRC safety requirements.

**Facility Safety Head (FSH)** – An appointed individual who is responsible for providing the Facility Team direction, obtaining required support from knowledgeable research personnel, and approving all CCDs affecting the facility.

**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** – 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 Configuration Controlled Documents (CCDs) for a LaRC facility during the initial Systems Safety Analysis or any subsequent upgrade effort. The team is composed of the FSH, FC, FCC, SFAB FSSE, and SFAB FSWSE assigned to the System Safety effort and the Configuration Management (CM) Representative.

**Field Verified (or Field Verification)** – The process by which the accuracy of a CCD 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 or Field Verification relating to electrical work refer to LPR 1710.6, “Electrical Safety,” definitions 1.2.9 and 1.2.10.

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

**Job Hazard Analysis (JHA)** – A safety assessment technique that separates the job into steps, identifies the hazards associated with each step, and provides steps to eliminate or control identified hazards in each step (see LPR 8717.1, Job Hazard Analysis Program).

**Langley Operating Procedure (LOP)** – Detailed, written, step-by-step instruction to be routinely followed in operating a facility. LOPs contain all of the information considered pertinent to safe and efficient operation of the facility. LOPs are the basis, in part, for the Langley Risk Evaluation (LRE). LOPs may also be used for training operator personnel. LOPs are under the control of the CM Program.

**Langley Risk Evaluation (LRE)** – A safety analysis completed under the authority of the Langley Risk Evaluation Program (LREP).

**Langley Risk Evaluation Program (LREP)** – A program designed to provide Langley Risk Evaluations (LREs) and Langley Operating Procedures (LOPs) to selected equipment at LaRC which are not in the CM Program and not covered with a Safety Permit.

**Pressure Systems Configuration Management (PSCM) Program** – A program to continuously update the In-service Inspection/Recertification effort.

**Project Manager (PM)** – The engineer assigned by PEB 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 CM 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 (i.e., 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 considered safety-critical if it (1) causes or contributes to a hazard; (2) provides control or mitigation for hazards; (3) controls safety-critical functions; (4) processes safety-critical commands or data; (5) detects and reports, or takes corrective action if the system reaches a specific hazardous state; or (6) mitigates damage if a hazard occurs. References: NASA-STD-8719.13B, *NASA Software Safety Standard*, §4.1.1.2; NASA-GB-8719.13 *NASA Software Safety Guidebook*, §2.1.3 What is Safety-Critical Software?

**Safety Manager, SFAB, SMAO** – This individual reviews and approves all System Safety Analyses and reviews all changes to the SARs, SOPs, and checklists under the CM Program.

**Single Point Failure** – A discrete system element and/or interface, the malfunction and/or failure of which, taken individually, would cause failure of the entire system.

**Software** – “Software is defined as the computer programs, procedures, scripts, rules, and associated documentation and data pertaining to the development and operation of a computer system. Software includes programs and data. This definition includes commercial-off-the-shelf (COTS) software, government-off-the-shelf (GOTS) software, modified-off-the-shelf (MOTS) software, reused software, auto generated code, embedded software, firmware, and open source software components.”, NPR 7150.2A *NASA Software Engineering Requirements*, §P.1 Purpose

**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 CM Program.

**Standard Practice Engineer (SPE) for Pressure Systems** – An agent of the Pressure Systems Committee responsible for ensuring ground-based pressure systems comply with this document.

**Supporting Facility Documents (SFDs)** – Those documents identified on the SFD list that are considered part of the baseline documentation, but that do not meet the criteria for CCDs.

**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.

**Undesired Events List** – A listing in the SAR of system failures/malfunctions derived from the preliminary hazard analysis that could, if not adequately controlled, result in an undesired event.

**Working Masters** – Copies of the latest-revision CCDs (SARs, SACRs, SOPs, drawings, and so forth), which are stamped “WORKING MASTER” in red and kept at the facility.

**APPENDIX B. ACRONYMS**

CCD	Configuration Controlled Documentation
CDR	Critical Design Review
CM	Configuration Management
CMOL	Configuration Management On-Line
CNS	Change Notification Sheet
CoF	Construction of Facility
COD	Center Operations Directorate
COTS	Commercial-Off-the Shelf
CP	Center Procedure
CSI	Computer System Inventory
CSIL	Computer System Inventory List
DAS	Data Acquisition System
EC	Effort Code
EDF	Engineering Drawing Files
EPA	Environmental Protection Agency
FBL	Facility Baseline List
FC	Facility Coordinator
FCC	Facilities Configuration Coordinator
FM	Facility Manager
FRI	Facility Risk Indicator
FSCM	Facility Software Configuration Manager
FSE	Facility Systems Engineer
FSH	Facility Safety Head
FSSA	Facility Systems Safety Analysis
FSSE	Facility System Safety Engineer
FSWSE	Facility Software Safety Engineer
FV	Field Verified
GOTS	Government-Off-the-Shelf
HA	Hazard Analysis
IH	Industrial Hygienist
ISR	Integrated System Review
JHA	Job Hazardous Analysis
LAPD	Langley Policy Directives
LaRC	Langley Research Center
LF	Langley Form
LMS	Langley Management System
LOP	Langley Operating Procedure
LPR	Langley Procedure Requirement
LRE	Langley Risk Evaluation

LREP	Langley Risk Evaluation Program
MOTS	Modified-Off-the-Shelf
NPR	NASA Procedural Requirement
OP	Operational Procedure
ORR	Operational Readiness Review
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	Personnel Protective Equipment
PR	Pre-Operational Procedure
PSCM	Pressure Systems Configuration Management
PSD	Pressure Systems Document
RAC	Risk Assessment Code
SA	Software Assurance
SACR	Software Assurance Classification Report
SAR	Safety Analysis Report
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCR	Software Change Request
SFAB	Safety and Facility Assurance Branch
SFD	Supporting Facility Document
SMAO	Safety and Mission Assurance Office
SPE	Standard Practice Engineer
SOP	Standard Operating Procedure

## APPENDIX C. FACILITY RISK INDICATOR (FRI)

### C.1 Purpose of LaRC FRIs

- a. The LaRC FRI is the initial safety assessment used to help determine the level of system safety effort required for a facility to meet NASA-LaRC safety requirements. The primary objective of the FRI is to qualitatively identify potential hazards associated with the facility and to ensure that the proper system safety effort is performed for that facility. By considering the size and complexity of the facility and the hazards associated with it, this assessment will help identify the system safety activities that shall be accomplished in order to ensure the safety of public, personnel, and property at LaRC. There are four FRIs, ranging from a FRI of 1 to a FRI of 4. The potential hazards inherent to the facility are evaluated using the following criteria as evaluation factors:
  - 1) **Public Safety** – hazards that could potentially harm the public in any form or manner.
  - 2) **Life Safety** – hazards that could potentially cause death or serious injury to personnel.
  - 3) **Facilities Protection** – failures that could cause serious damage to facilities or equipment resulting in significant financial loss.
  - 4) **Environmental Damage** – hazards that could potentially harm the environment in any form or manner.

### C.2 FRI Assessment Classification

- a. All LaRC facilities shall be assigned an FRI from 1 to 4, based on identified potential hazards present in the facility, and their impact on Public Safety, Life Safety, and Facilities Protection.
- b. An FRI shall be given to a new facility prior to the start of research activities in that facility.
- c. Also, FRI shall be re-evaluated prior to the start of research activities at an existing facility that has undergone a CoF modification or prior to any existing facility being re-occupied by Langley employees. Buildings strictly used for office work are considered a facility in their entirety.
- d. The following definitions shall be used to classify LaRC facilities and the suggested safety activities warranted after the assignment of the FRIs.

#### C.2.1 FRI 1 (High Risk)

- a. Definition – There is a HIGH risk that identified potential hazards in this facility could cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more people, an occupational injury or illness resulting in a restricted workday or OSHA recordable incident, a first aid incident, damage to equipment or property in excess of \$1,000,000, or any injury/property damage to the public.
- b. Suggested Safety Program Requirements:
  - 1) Placement in the Facility Configuration Management Program.

- c. All utility facilities (e.g., substations, sewage plants) are classified with an FRI of 1. Any other facility that has been determined by SFAB to have an inherent high risk associated with it may also be classified with an FRI of 1.

### **C.2.2 FRI 2 (Moderate Risk)**

- a. Definition – There is a MODERATE risk that identified potential hazards in this facility could cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more people, an occupational injury or illness resulting in a restricted workday or OSHA recordable incident, a first aid incident, or damage to equipment or property from \$250,000 to \$1,000,000.
- b. Suggested Safety Program Requirements:
  - 1) Placement in the Langley Risk Evaluation Program.
- c. Any other facility that has been determined by SFAB to have an inherent moderate risk hazard associated with it may also be classified with an FRI of 2.

### **C.2.3 FRI 3 (Low Risk)**

- a. Definition – There is a LOW risk that identified potential hazards in this facility could cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more people, an occupational injury or illness resulting in a restricted workday or OSHA recordable incident, a first aid incident, or damage to equipment or property from \$1,000 to \$250,000.
- b. Suggested Safety Program Requirements:
  - 1) Perform a Job Hazard Analysis for all hazardous facility operations.
  - 2) Adherence to applicable codes, standards, and regulations.
- c. Any facility that contains some form of a shop (e.g., machine, pipe fitting, HVAC) is classified with an FRI of 3. Cooling towers at LaRC are considered to have an FRI of 3. Any other facility that has been determined by SFAB to have an inherent low risk hazard associated with it may also be classified with an FRI of 3.

### **C.2.4 FRI 4 (Very Low Risk)**

- a. Definition – There is a VERY LOW risk that identified potential hazards in this facility could cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more people, an occupational injury or illness resulting in a restricted workday or OSHA recordable incident, a first aid incident, or damage to equipment or property less than \$1,000.
- b. Suggested Safety Program Requirements:
  - 1) Adherence to applicable codes, standards, and regulations.
- c. Any facility that is solely used for office space is classified with an FRI of 4. All vacated and abandoned facilities are classified with an FRI of 4. Any other facility that has been determined by SFAB to have an inherent very low risk hazard associated with it may also be classified with an FRI of 4.

## **APPENDIX D. REQUIREMENTS FOR DEVELOPING SOPs/CHECKLISTS**

### **D.1 INTRODUCTION**

- D.1.1** The purpose of this instruction is to establish the procedures for the development, implementation, and revision of SOPs in a standardized format.
- D.1.2** This instruction 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 accident or incident due to operator error.
- D.1.3** This instruction should be closely followed when developing SOPs for new facilities. Deviations from this instruction may be permitted to enhance clarity but must be approved by the FSH, the FC, the Certified Operators, and the SFAB.
- D.1.4** It is not the intent of these instructions to require a re-write of all existing SOPs. A total re-write of SOPs for existing facilities could cause unnecessary confusion and may increase rather than decrease risk associated with facility operations.

### **D.2 GENERAL**

- D.2.1** For the purpose of this instruction, 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.
- D.2.2** 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.

### **D.3 PRE-OPERATIONAL**

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.

#### **D.4 OPERATIONAL**

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.

#### **D.5 POST-OPERATIONAL**

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

#### **D.6 TASK AND/ OR SUB-TASKS**

- D.6.1 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.
- D.6.2 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).

#### **D.7 LINE ITEMS OR STEPS**

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 1740.7) 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.



## D.8 FLOW SEQUENCE DETERMINATION

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.

## D.9 STANDARDIZATION

### D.9.1 TASK IDENTIFICATION

D.9.1.1 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 CM Program.
- b. “PR” Identifies the task as a Pre-Operational Procedure (PR), an Operational Procedure (OP) or a Post-Operational Procedure (PO).

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:

- 1) AIP (Alarm/Alarm/Response Policy),
- 2) IDSP (Instrumentation and Data System Procedure).
- 3) IOP (Integrated Operating Procedure),
- 4) MIP (Maintenance Instruction Procedure),
- 5) MOP (Maintenance Operating Procedure),
- 6) PMP (Preventative Maintenance Procedure), and
- 7) 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).

**D.9.1.2 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 Document", should be entered at the top center of each page. Page number should be bottom, centered, 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."

**D.9.1.3 STEP FORMAT**

D.9.1.3.1 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 1.4.

#### **D.9.1.4 NOTES, CAUTIONS, AND WARNINGS**

D.9.1.4.1 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

**D.9.1.5 CHECKLISTS**

- D.9.1.5.1 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 CCD and used every time the facility/ system is operated.
- D.9.1.5.2 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.
- D.9.1.5.3 An example of a complicated task would be the preheating of the 20" SWT. In this task, the preheat pressure is close to the pressure that will lift relief devices. If the SOPs are not expressly followed, the pressure may overshoot and cause the relief devices to lift. Although lifting safety devices is not a safety problem, it is not desirable. The checklist for this task would likely be an abbreviated, one-to-one, less-detailed instruction of the SOP.
- D.9.1.5.4 An example of a routine task would be establishing cooling water flow to a piece of equipment. In this task, the many steps to open valves may be omitted from the checklist and replaced with a single step. The step may read "Verify Cooling Water established." Verification could be observing an indicator light that is activated by a flow switch.

D.9.1.5.5 The following list further establishes instructions for generation of checklists:

- a. A checklist is a CCD document and requires generation of a CNS for modification.
- b. Checklist Format

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

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 E. RECORDS**

- E.1 All Federal employees 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)
  - d) Configuration Controlled Documentation
  - e) Engineering Drawing File(s)
  - f) Pressure Systems Document(s)
  - g) Langley Risk Evaluation(s)
  - h) Software Configuration Management Plan(s)
  - i) Software Assurance Classification Report(s)