# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td>3</td>
</tr>
<tr>
<td>P.1 PURPOSE</td>
<td>3</td>
</tr>
<tr>
<td>P.2 APPLICABILITY</td>
<td>3</td>
</tr>
<tr>
<td>P.3 AUTHORITY</td>
<td>3</td>
</tr>
<tr>
<td>P.4 APPLICABLE DOCUMENTS AND FORMS</td>
<td>3</td>
</tr>
<tr>
<td>P.5 MEASUREMENT/VERIFICATION</td>
<td>4</td>
</tr>
<tr>
<td>P.6 CANCELLATION</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 1.0 – FACILITY SYSTEM SAFETY PROGRAM</td>
<td>5</td>
</tr>
<tr>
<td>1.1 INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td>1.2 OBJECTIVES</td>
<td>5</td>
</tr>
<tr>
<td>1.3 DEFINITIONS</td>
<td>5</td>
</tr>
<tr>
<td>1.4 WAIVERS</td>
<td>6</td>
</tr>
<tr>
<td>CHAPTER 2.0 – FACILITY SYSTEM SAFETY ANALYSIS</td>
<td>7</td>
</tr>
<tr>
<td>2.1 PROGRAM SUMMARY</td>
<td>7</td>
</tr>
<tr>
<td>2.2 PLANNING AND EXECUTION</td>
<td>8</td>
</tr>
<tr>
<td>2.3 SOPs AND CHECKLISTS</td>
<td>8</td>
</tr>
<tr>
<td>2.4 SOP DEVELOPMENT REQUIREMENTS</td>
<td>9</td>
</tr>
<tr>
<td>2.5 SAFETY ANALYSIS REPORTS (SARS)</td>
<td>12</td>
</tr>
<tr>
<td>2.6 LARC INTERLOCK PHILOSOPHY</td>
<td>21</td>
</tr>
<tr>
<td>2.7 CRITERIA FOR DESIGNATING CONFIGURATION CONTROLLED ITEMS (CCIs)</td>
<td>23</td>
</tr>
<tr>
<td>CHAPTER 3.0 – RISK AND SAFETY REVIEW</td>
<td>24</td>
</tr>
<tr>
<td>3.1 ANNUAL SAFETY MEETINGS</td>
<td>24</td>
</tr>
<tr>
<td>3.2 PROCEDURE DEMONSTRATIONS</td>
<td>24</td>
</tr>
<tr>
<td>3.3 CONTINUAL FACILITY SYSTEM SAFETY ENGINEERING ANALYSES</td>
<td>24</td>
</tr>
<tr>
<td>APPENDIX A. DEFINITIONS</td>
<td>25</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 2-1. SAR Preparation Sequence........................................................................ 15
Figure 2-2. Risk Assessment Matrix .......................................................................... 19
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 Programs for the Center’s ground-based research facilities. It defines the requirements of the Center’s Facility System Safety Analysis Program. 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

P.4 APPLICABLE DOCUMENTS AND FORMS
c. NPD 1440.6, NASA Records Management.
g. LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects.
h. LPR 1710.42, Safety Program for the Recertification and Maintenance of Ground-Based Pressure Vessels and Piping Systems.
i. LPR 1710.6, Electrical Safety.
j. LPR 1740.2, Facility Safety Requirements.
k. LPR 1740.6, Personnel Safety Certification.
l. LPR 7123.2, Facility Configuration Management.
m. LAPD 7150.10, Facility Software Classification Policy.
n. LMS-CP-4710, Facility Change Request Process.
o. LMS-CP-7151, Obtaining Waivers for Langley Management System (LMS) Requirements.
p. LMS-CP-8715, Facility Risk Tier Determination.

P.5 MEASUREMENT/VERIFICATION
None

P.6 CANCELLATION
LPR-1740.4L, dated May 19, 2010
LPR-1740.4M, dated May 3, 2013
LPR-1740.4N, dated October 11, 2015
CID-1740.4N, dated August 19, 2016

/s/ Cathy Mangum March 9, 2018
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 a Facility System Safety Analysis (FSSA).
   b. Facility Configuration Management (FCM) per LPR 7123.2:
      (1) Facility Configuration Management (CM) Program,
      (2) Pressure Systems Configuration Management (PSCM),
      (3) Software Configuration Management (SCM),

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 facility configuration management per LPR 7123.2, 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, are to:
   a. Identify hazards,
   b. Determine the risk of hazards in terms of severity and probability,
   c. Assess the controls for those hazards, and
   d. Recommend controls that will eliminate the hazard or reduce the risk of the hazard.

1.2.3 The objectives of a safety-critical software analysis are to:
   a. 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, and
   d. Ensure software risk mitigations and software hazard causations are duly considered during the FSSA or LRE.

1.3 DEFINITIONS
1.3.1 The glossary in Appendix A lists and defines the terms unique to Facility System Safety program.
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 facility configuration management 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 Controlled Items (CCI),

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 Configuration Management Owner (FCMO),

c. Facility Systems Engineer (FSE),

d. Facility Safety Head (FSH),

e. Facility Coordinator (FC),
f. Facility Software Configuration Manager (FSCM),
g. Facility System Safety Engineer (FSSE) from SFAB,
h. Facility Software Safety Engineer (FSWSE) from SFAB

2.1.6 The above members of a Facility Team are permanent members who also assist with meeting the requirements of the 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-built" 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 and SOPs and identify CCIs are discussed in Sections 2.3, 2.4, 2.5, and 2.7. Details to develop the SACR and CCIs are covered in LPR 7123.2.

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.

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 C, 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; however, if a facility chooses to have checklists they must be demonstrated, approved, and brought under FCM prior to their use.

d. Checklists shall be developed in accordance with Appendix C, 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 CCIs, they shall be changed and distributed in accordance with the requirements set forth in per LPR 7123.2.
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 2.5.3.

2.5.2 The SAR shall be a CCI 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 or real property asset number (e.g. B1250 or 880-10 for Fire Alarm Systems) in which the facility is housed.

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

(5) The "Facility Owner/Supervisor" row shall be signed by the Supervisor of the 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 CCIs, they shall be changed and distributed in accordance with the requirements set forth in LPR 7123.2.

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

Verify the correct version before use by checking the LMS Web site.
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 Facility Configuration Management (FCM) 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.

---

**Figure 2-2. Risk Assessment Matrix**

Verify the correct version before use by checking the LMS Web site.
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 FCM in accordance with LPR 7123.2. At no time shall software changes be made while the facility is online (i.e., in operation).

g. Bypassing safety interlocks or devices during facility operation (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.

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 CONFIGURATION CONTROLLED ITEMS (CCIs)

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 drawings, documents, and models (Building Information Models (BIM)) as CCI and placing these in the Facility CM Program per LPR 7123.2. CCI are generally designated as such when they provide the following:

a. Support of the conclusions of the safety analysis or
b. Support the effective troubleshooting of systems (e.g., electrical, computer, mechanical).
CHAPTER 3.0 – 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.

3.1 ANNUAL SAFETY MEETINGS

3.1.1 Annual Safety Meetings are held for each LaRC facility. These meetings are scheduled by an SFAB Representative.

3.1.2 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.

3.2 PROCEDURE DEMONSTRATIONS

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

a. FSH
b. FCM Owner representative
c. Certified Operator(s)
d. SFAB Representative

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

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

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

3.3 CONTINUAL FACILITY SYSTEM SAFETY ENGINEERING ANALYSES

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

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

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

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

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

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

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

Facility Configuration Management (FCM) 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 FCR Form.

**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 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 CCIs 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 Items (CCIs) for a LaRC facility during the initial Systems Safety Analysis or any subsequent upgrade effort. The team is composed of the FSH, FC, FCMO, 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 CCI or any other drawing is verified. That accuracy is attested to by affixing a “Field Verified” statement, signed by the person doing the verification, and signed and dated by the Project Engineer, FSH, or FC. NOTE: For Field Verified 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 1740.2).

**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-8719.13, 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 7150.2 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 CCIs.

**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 CCIs (SARs, SACRs, SOPs, drawings, and so forth), which are stamped “WORKING MASTER” in red and kept at the facility.
# APPENDIX B. ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIM</td>
<td>Building Information Model</td>
</tr>
<tr>
<td>CCI</td>
<td>Configuration Controlled Item</td>
</tr>
<tr>
<td>CDR</td>
<td>Critical Design Review</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>CoF</td>
<td>Construction of Facility</td>
</tr>
<tr>
<td>COD</td>
<td>Center Operations Directorate</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial-Off-the Shelf</td>
</tr>
<tr>
<td>CP</td>
<td>Center Procedure</td>
</tr>
<tr>
<td>CSI</td>
<td>Computer System Inventory</td>
</tr>
<tr>
<td>CSIL</td>
<td>Computer System Inventory List</td>
</tr>
<tr>
<td>DAS</td>
<td>Data Acquisition System</td>
</tr>
<tr>
<td>EC</td>
<td>Effort Code</td>
</tr>
<tr>
<td>EDF</td>
<td>Engineering Drawing Files</td>
</tr>
<tr>
<td>EPA</td>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>FBL</td>
<td>Facility Baseline List</td>
</tr>
<tr>
<td>FC</td>
<td>Facility Coordinator</td>
</tr>
<tr>
<td>FCM</td>
<td>Facility Configuration Management</td>
</tr>
<tr>
<td>FCMO</td>
<td>Facility Configuration Management Owner</td>
</tr>
<tr>
<td>FCR</td>
<td>Facility Change Request</td>
</tr>
<tr>
<td>FM</td>
<td>Facility Manager</td>
</tr>
<tr>
<td>FRI</td>
<td>Facility Risk Indicator</td>
</tr>
<tr>
<td>FSCM</td>
<td>Facility Software Configuration Manager</td>
</tr>
<tr>
<td>FSE</td>
<td>Facility Systems Engineer</td>
</tr>
<tr>
<td>FSH</td>
<td>Facility Safety Head</td>
</tr>
<tr>
<td>FSSA</td>
<td>Facility Systems Safety Analysis</td>
</tr>
<tr>
<td>FSSE</td>
<td>Facility System Safety Engineer</td>
</tr>
<tr>
<td>FSWSE</td>
<td>Facility Software Safety Engineer</td>
</tr>
<tr>
<td>FV</td>
<td>Field Verified</td>
</tr>
<tr>
<td>GOTS</td>
<td>Government-Off-the-Shelf</td>
</tr>
<tr>
<td>HA</td>
<td>Hazard Analysis</td>
</tr>
<tr>
<td>IH</td>
<td>Industrial Hygienist</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>ISR</td>
<td>Integrated System Review</td>
</tr>
<tr>
<td>JHA</td>
<td>Job Hazardous Analysis</td>
</tr>
<tr>
<td>LAPD</td>
<td>Langley Policy Directives</td>
</tr>
<tr>
<td>LaRC</td>
<td>Langley Research Center</td>
</tr>
<tr>
<td>LF</td>
<td>Langley Form</td>
</tr>
<tr>
<td>LMS</td>
<td>Langley Management System</td>
</tr>
<tr>
<td>LPR</td>
<td>Langley Procedure Requirement</td>
</tr>
<tr>
<td>MOTS</td>
<td>Modified-Off-the-Shelf</td>
</tr>
<tr>
<td>NPR</td>
<td>NASA Procedural Requirement</td>
</tr>
<tr>
<td>OP</td>
<td>Operational Procedure</td>
</tr>
<tr>
<td>ORR</td>
<td>Operational Readiness Review</td>
</tr>
<tr>
<td>PDR</td>
<td>Preliminary Design Review</td>
</tr>
<tr>
<td>PEB</td>
<td>Project and Engineering Branch</td>
</tr>
<tr>
<td>PHA</td>
<td>Preliminary Hazard Analysis</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PM</td>
<td>Project Manager</td>
</tr>
<tr>
<td>PO</td>
<td>Post-Operational Procedure</td>
</tr>
<tr>
<td>PPE</td>
<td>Personnel Protective Equipment</td>
</tr>
<tr>
<td>PR</td>
<td>Pre-Operational Procedure</td>
</tr>
<tr>
<td>PSCM</td>
<td>Pressure Systems Configuration Management</td>
</tr>
<tr>
<td>PSD</td>
<td>Pressure Systems Document</td>
</tr>
<tr>
<td>RAC</td>
<td>Risk Assessment Code</td>
</tr>
<tr>
<td>SA</td>
<td>Software Assurance</td>
</tr>
<tr>
<td>SACR</td>
<td>Software Assurance Classification Report</td>
</tr>
<tr>
<td>SAR</td>
<td>Safety Analysis Report</td>
</tr>
<tr>
<td>SCM</td>
<td>Software Configuration Management</td>
</tr>
<tr>
<td>SCMP</td>
<td>Software Configuration Management Plan</td>
</tr>
<tr>
<td>SCR</td>
<td>Software Change Request</td>
</tr>
<tr>
<td>SFAB</td>
<td>Safety and Facility Assurance Branch</td>
</tr>
<tr>
<td>SFD</td>
<td>Supporting Facility Document</td>
</tr>
<tr>
<td>SMAO</td>
<td>Safety and Mission Assurance Office</td>
</tr>
<tr>
<td>SPE</td>
<td>Standard Practice Engineer</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
</tbody>
</table>
APPENDIX C. REQUIREMENTS FOR DEVELOPING SOPS/CHECKLISTS

C.1 INTRODUCTION

C.1.1 The purpose of this instruction is to establish the procedures for the development, implementation, and revision of SOPs in a standardized format.

C.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.

C.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 SFAB.

C.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.

C.2 GENERAL

C.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.

C.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.

C.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.
C.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.

C.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.

C.6 TASK AND/OR SUB-TASKS

C.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.

C.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).

C.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 1740.6) to safely operate the facility/system. Each line item or step should be signed-off/initialed by the certified operator performing that step. Steps that have been deemed “Not Applicable” by a certified operator should be signed-off/initialed by the Facility Safety Head, including the date of the approval.

C.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.
C.9 STANDARDIZATION

C.9.1 TASK IDENTIFICATION

C.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).

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

C.9.1.3 STEP FORMAT

C.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.
C.9.1.4 NOTES, CAUTIONS, AND WARNINGS

C.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

C.9.1.5 CHECKLISTS

C.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 CCI and used every time the facility/system is operated.

C.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.

C.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.

C.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.

C.9.1.5.5 The following list further establishes instructions for generation of checklists:
a. A checklist is a CCI document and requires generation of a FCR for modification.

b. Checklist Format

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

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

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

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

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

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

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

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

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

D.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.

D.2 Identified documents:
   a. Standard Operating Procedure(s)
   b. Checklist(s)
   c. Safety Analysis Report(s)