Langley Research Center

Directives Management

Transmittal Sheet

October 6, 2009

Material Transmitted

Revision / modification

LPR 1740.4, Facility System Safety Analysis and Configuration Management

Summary

This directive is undergoing review per CP 1401, Langley Management System Document Control to approve a status transfer from CID to LPR.

The material has been reviewed by the owning organization, SMAO, with the following outcome(s):

1. Figure 1-1, Effort Code Summary updated
2. Figure 6.1 added: Equipment/Operations LREP Energy Source Levels
3. Section 1: Additional/refined objectives for Configuration Management Programs
4. Sections 2.4.1; 2.4.2: New requirement provided in Appendix D, Requirements for Developing SOPs/Checklists
5. Sections 2.4.3.1(e) & (f); 2.4.3.3 and 2.4.4: requirements for writing/preparing elements of SOPs/Checklists

Langley Research Center

LPR 1740.4

Effective Date: TBD

Expiration Date: TBD

FACILITY SYSTEM SAFETY ANALYSIS AND CONFIGURATION MANAGEMENT

National Aeronautics and Space Administration

Responsible Office: Safety and Mission Assurance Office

PREFACE

P.1 PURPOSE

a. This Langley Procedural Requirement (LPR) implements the requirements of NASA Procedural Requirement (NPR) 8715.3C, "NASA General Safety Program Requirements (w/Change 4 dated 7/20/09~~3~~)." and is part of the Langley Management System (LMS). This LPR sets forth procedural requirements for the Langley Research Center (LaRC) Facility System Safety 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 personnel in performing their responsibilities for these programs.

P.2 APPLICABILITY

a. This LPR is applicable to all Langley employees.

P.3 AUTHORITY

a. NPR 8715.3C, "NASA General Safety Program Requirements (w/Change 4 dated 7/20/09~~3~~)."

P.4 REFERENCES

a. NASA-STD-8719.7, "Facility System Safety Guidebook"
b. LAPD 1700.2, Safety Assignments
c. LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects
d. LPR 1710.42, Safety Program for Maintenance of Ground-Based Pressure Vessels and Pressurized Systems
e. LPR 1740.2, Facility Safety Requirements
f. LPR 1740.3, Facility Safety Head and Facility Coordinator Guide
g. LPR 1740.7, Process Systems Certification Program
h. LPR 8717.1, Job Hazard Analysis Program
i. LMS-CP-4710, Configuration Management for Facilities
j. LMS-CP-4890, Construction and Change Assurance for High Risk Facilities
k. LMS-CP-5528, Software Planning, Development, Acquisition, Maintenance, and Operation
l. LMS-CP-5529, Software Configuration Management Planning for Low-, High-, and Critical-Control Software
m. LMS-OP-8715, Identifying Facility Risk Indicators

P.5 RECORDS

a. NASA Langley Form 27, ~~"~~NASA LaRC Asbestos Safety Permit~~"~~,
b. NASA Langley Form 127, Change Notification Sheet
c. NASA Langley Form 275, Job Hazard Analysis Worksheet
d. NASA Langley Form 445, Facility Risk Indicator (FRI) Identification Form
e. Standard Operating Procedures
f. Checklist
g. Safety Analysis Report
h. Configuration Controlled Documentation
i. Engineering Drawing Files
j. Pressure Systems Configuration Management Revision Record
k. Langley Risk Evaluation
l. Asbestos Configuration Management Report

P.6 CANCELLATION

a. CID 1740.4, dated November 17, 2008

Lesa B. Roe
Director

~~DISTRIBUTION:~~
~~305/Safety and Facility Assurance Branch, Safety and Mission Assurance Office (25 copies)~~

TABLE OF CONTENTS

Chapter **Page**

1. FACILITY SYSTEM SAFETY PROGRAM 1
1.1 Introduction 1
1.2 Objectives 5
1.3 Definitions 6

2. FACILITY SYSTEM SAFETY ANALYSIS 1
2.1 PROGRAM SUMMARY 1
2.2 Planning and Execution 2
2.3 SOP'S and Checklists 2
2.4 SOP Development Requirements 2
2.4.2 Checklist Development Requirements 3
2.4.3 SOP/Checklist Organization 4
2.4.3.1Introductory Matter 4
2.4.3.2Text 5
2.4.3.3Emergency Procedures 5
2.4.4 Changes to SOP's/Checklists developed before LPR Effective Date 5
2.4.5 SOP's/Checklists Changes and Distribution 6
2.5 SAFETY ANALYSIS REPORTS (SAR's) 6
2.5.1 SAR Organization 6
2.5.1.1Introductory Matter 6
2.5.1.2Text 7
2.5.1.3Appendices 7
2.5.1.4Critical Items List (CIL) 7
2.5.1.5SAR Changes and Distribution 7
2.5.2 SAR Preparation 7
2.5.2.1 Phases 8
2.5.3 Hazard Analysis 11
2.5.4 Risk Assessment 14
2.5.4.1 Severity Category 14
2.5.4.2 Probability of Occurrence Level 14
2.5.4.2 Establishing a Risk Assessment Code (RAC) 15
2.5.4.3 Implications of a Given RAC 15
2.6 LaRC INTERLOCK PHILOSOPHY 16
2.6.1 Design 17
2.6.2 Engineered Safety Features 17
2.6.3 Safety Devices / Personal Protective Equipment 17
2.6.4 Warning Devices 18
2.6.5 Procedures/Training 18
2.7 CRITERIA FOR DESIGNATING DRAWINGS AS CCD's 18

3. FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM 1
3.1 PROGRAM SUMMARY 1
3.2 CHANGE CONTROL 1

3.3 UPDATING AND DISTRIBUTING CCD 2
3.4 TYPES OF CHANGE 2
3.4.1 Administrative Change 3
3.4.2 No Safety Impact 3
3.4.3 Safety Impact 3
3.4.4 Change Controlled by Design Review Process 4
3.5 CONFIGURATION CONTROL DOCUMENTATION – DRAWINGS 4
3.5.1 Drawing Field Verification 4
3.5.2 Changes to CCD Drawings 5
3.5.3 Working Masters 5
3.6 FACILITY BASELINE LIST (FBL) AND SUPPORTING FACILITY DOCUMENTS 6
3.7 FILING SYSTEMS FOR CCD's 6
3.7.1 Engineering Drawing Files (EDF) 6
3.7.2 Facility Files 7
3.8 RISK AND CM REVIEW 7
3.8.1 Annual CM Meetings 7
3.8.2 Procedure Demonstrations 7
3.8.3 Continual Facility System Safety Engineering Analyses 7
3.9 CONFIGURATION MANAGEMENT ON-LINE (CMOL) 8
3.9.1 Access and Database Maintenance 8
3.9.2 CNS Initiation/Processing 8

4. PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM) 1
4.1 PROGRAM SUMMARY 1
4.2 PRESSURE SYSTEMS DOCUMENT (PSD) 2

5. FACILITY SOFTWARE ASSURANCE AND CONFIGURATION MANAGEMENT 1
5.1 GENERAL 1
5.2 PROGRAM OVERVIEW 1

6. LANGLEY RISK EVALUATION PROGRAM (LREP) 1
6.1 PROGRAM SUMMARY 1
6.2 LANGLEY RISK EVALUATIONS (LRE's) 2
LREP CHANGES AND DISTRIBUTION 3

7. ASBESTOS CONFIGURATION MANAGEMENT 1
7.1 PROGRAM SUMMARY 1
7.2 ASBESTOS CONFIGURATION MANAGEMENT REPORTS 2
7.3 ASBESTOS CM CHANGES 2

~~1 FACILITY SYSTEM SAFETY PROGRAM ..... 1-1~~
~~1.1 Introduction ..... 1-1~~
~~1.2 Objectives ..... 1-3~~
~~1.3 Definitions ..... 1-3~~

~~2 FACILITY SYSTEM SAFETY ANALYSIS ..... 2-1~~
~~2.1 Program Summary ..... 2-1~~
~~2.2 Planning And Execution ..... 2-2~~

~~2.3 SOP's And Checklists ..... 2-2~~
~~2.3.1 SOP Guidelines ..... 2-2~~
~~2.3.2 Checklist Guidelines ..... 2-3~~
~~2.3.3 SOP/Checklist Organization ..... 2-3~~
~~2.3.3.1 Introductory Matter ..... 2-3~~
~~2.3.3.2 Text ..... 2-4~~
~~2.3.4 SOP's/Checklists Changes and Distribution ..... 2-4~~
~~2.4 Safety Analysis Reports (SAR's) ..... 2-4~~
~~2.4.1 SAR Organization ..... 2-4~~
~~2.4.1.1 Introductory Matter ..... 2-4~~
~~2.4.1.2 Text ..... 2-5~~
~~2.4.1.3 Appendices ..... 2-5~~
~~2.4.1.4 Critical Items List (CIL) ..... 2-5~~
~~2.4.1.5 SAR Changes and Distribution ..... 2-6~~
~~2.4.2 SAR Preparation ..... 2-6~~
~~2.4.2.1 Phases ..... 2-6~~
~~2.4.3 Hazard Analysis ..... 2-9~~
~~2.4.4 Risk Assessment ..... 2-11~~
~~2.4.4.1 Severity Category ..... 2-11~~
~~2.4.4.2 Probability of Occurrence Level ..... 2-11~~
~~2.4.4.3 Establishing a Risk Assessment Code (RAC) ..... 2-12~~
~~2.4.4.4 Implications of a Given RAC ..... 2-12~~
~~2.5 LaRC Interlock Philosophy ..... 2-13~~
~~2.5.1 Design ..... 2-14~~
~~2.5.2 Engineered Safety Features ..... 2-14~~
~~2.5.3 Safety Devices / Personal Protective Equipment ..... 2-14~~
~~2.5.4 Warning Devices ..... 2-14~~
~~2.5.5 Procedures/Training ..... 2-14~~
~~2.6 Criteria For Designating Drawings As CCD's ..... 2-14~~

~~**3 FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM ..... 3-1**~~
~~3.1 Program Summary ..... 3-1~~
~~3.2 Change Control ..... 3-1~~
~~3.3 Updating And Distributing Ccd ..... 3-2~~
~~3.4 Types Of Change ..... 3-2~~
~~3.4.1 Administrative Change ..... 3-2~~
~~3.4.2 No Safety Impact ..... 3-2~~
~~3.4.3 Safety Impact ..... 3-2~~
~~3.4.4 Change Controlled by Design Review Process ..... 3-3~~
~~3.5 Configuration Control Documentation - Drawings ..... 3-3~~
~~3.5.1 Drawing Field Verification ..... 3-4~~
~~3.5.1 Changes to CCD Drawings ..... 3-4~~
~~3.5.2 Working Masters ..... 3-4~~
~~3.6 Facility Baseline List (FBL) And Supporting Facility Documents ..... 3-5~~
~~3.7 Filing Systems For CCD's ..... 3-5~~
~~3.7.1 Engineering Drawing Files (EDF) ..... 3-5~~
~~3.7.2 Facility Files ..... 3-6~~

~~3.8 Risk And CM Review ..... 3-6~~
~~3.8.1 Annual Cm Meetings ..... 3-6~~
~~3.8.2 Procedure Demonstrations ..... 3-6~~
~~3.8.3 Continual Facility System Safety Engineering Analyses ..... 3-6~~
~~3.9 Configuration Management On-Line (CMOL) ..... 3-7~~
~~3.9.1 Access and Database Maintenance ..... 3-7~~
~~3.9.2 CNS Initiation/Processing ..... 3-7~~

~~4 **PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM)** ..... 4-1~~
~~4.1 Program Summary ..... 4-1~~
~~4.2 Pressure Systems Document (PSD) ..... 4-1~~

~~5 **FACILITY SOFTWARE ASSURANCE AND CONFIGURATION MANAGEMENT** ..... 5-1~~
~~5.1 General ..... 5-1~~
~~5.2 Program Overview ..... 5-1~~

~~6 **LANGLEY RISK EVALUATION PROGRAM (LREP)** ..... 6-1~~
~~6.1 Program Summary ..... 6-1~~
~~6.2 Langley Risk Evaluations (LRE's) ..... 6-2~~
~~6.3 Lrep Changes And Distribution ..... 6-2~~

~~7 **ASBESTOS CONFIGURATION MANAGEMENT** ..... 7-1~~
~~7.1 Program Summary ..... 7-1~~
~~7.2 Asbestos Configuration Management Reports ..... 7-1~~
~~7.3 Asbestos Cm Changes ..... 7-2~~

APPENDICES

Appendix **Page**

A. Glossary Of Key Terms.....A-1
B. Acronyms.....B-1
C. Facility Risk Indicator C-1

D. Requirements for Developing SOPs/Checklists..... D-1

LIST OF FIGURES

Page

FIGURE 1-1 Effort Code Summary 1-2
FIGURE 2-1 SAR Preparation Sequence 2-8
FIGURE 2-2 Risk Assessment Matrix..... 2-10
FIGURE 6-1 Equipment/Operations LREP Energy Source Levels 6-1

Chapter 1

1. 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 comprised of two major ~~components~~elements:

a. ~~safety analysis and configuration management.~~ A safety analysis which takes the form of either:

1. ~~-~~a Facility System Safety Analysis (FSSA) or
2. a Langley Risk Evaluation~~Langley Risk Evaluation~~

~~.~~

~~a.~~ b. and ~~LaRC's configuration~~ configuration management that includes ~~programs are as follows~~:

~~b.~~ Facility Configuration Management (CM) Program,

1.
2. Pressure Systems Configuration Management (PSCM),
3. Software Configuration Management (SCM),
4. Langley Risk Evaluation Program (LREP), and
5. Asbestos Configuration Management Program (ACMP).

~~c. Pressure Systems Configuration Management (PSCM),~~
~~d. Software Configuration Management (SCM),~~
~~e. Langley Risk Evaluation Program (LREP), and~~
~~f. Asbestos Configuration Management Program (ACMP).~~

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 have had 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. 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~~their~~ EC numbers are listed in Figure 1-1, "Effort Code Summary." ~~Most research facilities not in the Facility CM Program are included in the LREP, which provides a job hazard analysis (JHA) and risk evaluation of the equipment.~~

1.1.3 SFAB utilizes the ~~Facility Risk Indicator (~~FRI~~)~~ in determining whether a research facility or piece of research equipment is placed in the Facility Configuration Management Program or Langley Risk Evaluation Program. All research ~~F~~facilities at La~~A~~RC are given a FRI. The assessment criterion for assigning a FRI to a facility is

located in Appendix C. The operational procedure to assign a FRI in a facility may be found in LMS-OP-8715.

1.1.4 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 Facility System Safety Analysis process,
b. Chapter 3 addresses the Facility CM Program,
c. Chapter 4 addresses the PSCM Program,
d. Chapter 5 addresses the SCM Program,
e. Chapter 6 addresses the LREP, and
f. Chapter 7 addresses the ACMP.

EC	BLDG	FACILITY NAME
01	1247E	West Area High Pressure Air System
02	1275	20-Inch Mach 6~~Hypersonic~~ CF_4 Tunnel
03	1265	8-Foot High Temperature Tunnel
05		Hypersonic Blowdown Tunnels:
05-01	1247D	* 20” Mach 6 Tunnel
05-02	1247D	* Nozzle Test Chamber
~~05-05~~	~~1247D~~	~~* Gas Mixing Apparatus (Closed)~~
~~05-06~~	~~1247D~~	~~* 18” Mach 8 Tunnel~~
05-07	1247D	* Supersonic Low Disturbance Tunnel
05-08	1247D	* High Pressure Air and Vacuum Systems
05-09	1247D	* 20” Supersonic Wind Tunnel
05-10	1247D	* Probe Calibration Tunnel
05-11	1247D	* Grazing Flow Impedance Tube
05-12	1247D	* Curved Duct Test Rig
~~07~~	~~1247B~~	~~Hypersonic N_2 Tunnel (Closed)~~
13	1268A	Visual Motion Simulator
16	1251A	31-Inch Mach 10 Tunnel
17	1251A	15-Inch Mach 6 High Temperature Tunnel
18	648	Transonic Dynamics Tunnel
19	1212C	14- X 22-Foot Subsonic Tunnel
21	1234	Jet Exit Test Facility
22	1208	~~Aircraft Noise Reduction~~Acoustic Research Laboratory
23	1148B	Hypersonic Materials Test Apparatus
24	1251B	Unitary Wind Tunnel
25	1247B	Arc-Heated Scramjet Test Facility
29	1257/1262	Aircraft Landing Dynamics Facility
33	1297	~~Impact Dynamics~~Landing and Impact Research Facility
34	1242	0.3-Meter Transonic Cryogenic Tunnel
~~35~~	~~1218A~~	~~Anechoic Noise Facility~~
36	1221A	Jet Noise Apparatus
37	1221B	Thermal Acoustic Fatigue Apparatus
~~40~~	~~582A~~	~~Low Turbulence Pressure Tunnel (Closed)~~
53	1268A	Lunar Flight Deck
54	1268A	Developmental and Test Simulator
55	1268D	Cockpit Motion Facility
~~58~~	~~1275~~	~~Impact and Projectile Range (Closed)~~
61	644	12-Foot Low Speed Tunnel
62	645	20-Foot Vertical Spin Tunnel
66	1268A	Differential Maneuvering Simulator
71	1221D	Direct Connect Supersonic Combustion Test Facility~~Vitiated Heater~~, Test Cell #2
75	1256	Combined Loads Test System (COLTS) – Test Machine
80	1221D	Combustion Heated Scramjet Test Facility~~and Mixing Research Apparatus~~, Test Cell #1
84	1244	Hangar Foam Deluge System
85	1232A	Heavy-Duty Brazing Vacuum Furnace
86	1293B	16-Meter Thermal Vacuum Chamber
91	1238B	Composite Shop Autoclave
97	1293	Space Systems Structures Research Laboratory
98	1215	Steam Distribution System
99	1236	National Transonic Facility (NTF)
100	1241	Liquid Nitrogen Plant
300	1233	Switching Diagrams
301	Various	Manhole Drawings
302	Various	Low-Voltage One-Line Drawings
303	Various	Stratton Substation Control Diagrams
400	1205	Materials Research Laboratory
401	1225	Advanced Development Lab
402	1233	Stratton Road Substation
403	1250	Systems Integration & Test Branch

404	1267	Component Verification Facility

Figure 1-1, Effort Code Summary[MSOffice1].[JSP2]

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 ~~and provide the information~~ to management and ~~operating personnel~~employees.

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

a. To ~~I~~identify ~~credible~~ hazards,
b. To determine the risk~~Define the~~ of hazards in terms of severity and probability,
c. To ~~A~~assess the controls for those hazards, and
d. To recommend controls that will eliminate the hazard or reduce the risk~~Make recommendations toward reduction of the severity and/or probability of occurrence~~ of the hazard.~~.~~

1.2.3 The objectives of the Facility CM program:

a. Is to ~~R~~record and maintain safety analysis documentation,
b. Is to ~~D~~document and maintain standard operating procedures for use by operating personnel,
c. Is to ~~En~~ensure ~~the~~ SFAB reviews changes that affect safety, and
d. To ~~E~~establish and maintain a baseline for designated systems (e.g., electrical systems) and the relevant documentation (e.g., drawings).

1.2.4 The objectives of the Pressure Systems Configuration management Program:

a. Is to maintain the configuration of Pressure System Documents (PSD)

1.2.5 The objectives of the Software Configuration Management Program:

a. Is to document and maintain configuration control of software and,
b. Is to ensure SFAB reviews changes that affect safety

1.2.~~4~~6 The objectives of the Langley Risk Evaluation Program:

a. Is to ~~R~~record and maintain the risk evaluation,
b. Document and maintain JHAs for use by operating personnel

1.2.7 The objectives of the Asbestos Configuration Management Program:

a. Increase safety awareness and minimize the risk of asbestos exposure to personnel

b. Institute controls to prevent the release of asbestos fibers, restrict future asbestos use, and develop surveillance and control of known, existing asbestos applications in LaRC facilities.

~~**1.2.5 LaRC's PSCM and ACMP are special CM programs. The objective of the PSCM is to maintain the configuration of Pressure System Documents (PSD); these are documents that provide detailed information about a particular high pressure system. The objectives of the ACMP are: (1) increase safety awareness and minimize the risk of asbestos exposure to personnel and (2) institute controls to prevent the release of asbestos fibers, restrict future asbestos use, and develop surveillance and control of known, existing asbestos applications in LaRC facilities.**~~

1.3 Definitions

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

Chapter 2

2. FACILITY SYSTEM SAFETY ANALYSIS

2.1 PROGRAM SUMMARY

2.1.1 A Facility Systems Safety Analysis (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 prior to the start of research activities at a new facility, prior to the start of research activities at an existing facility that has undergone a Construction of Facility (CoF) modification or prior to any existing facility being brought into the Facility CM Program. The final documents of this effort, all of which shall be placed in the Facility CM Program, are

a. Standard Operating Procedures (SOP's) and Checklists,
b. Safety Analysis Report (SAR),
c. Configuration Control Documentation (CCD),
d. Other special items identified by the Facility Team.

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

2.1.4 The overall responsibility for conducting the FSSA lies with the Safety and Facility Assurance Branch (SFAB). However, the analysis is a group effort conducted by a Facility Team. A Facility Team includes:

a. Organizational Facility Safety Head (OFSH) (henceforth called FSH),
b. Facility Coordinator (FC),
c. Facilities Configuration Coordinator (FCC) from the Project and Engineering Branch (PEB),
d. Facility System ~~FSSE~~ SafetyEngineer (FSSE) from SFAB, and
e. Configuration Management (CM) Engineer from CM contractor.

2.1.5 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) [JSP3]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 will notify the responsible FSH about the initiation of a FSSA. The FSH, with the assistance of the facility staff ~~and technicians~~, will 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 SOP’s 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.

2.2.2 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, SOP’s, and identify CCD are discussed in the following paragraphs.

2.2.3 For new facilities or CoF projects, it is very important that the SFAB FSSE be involved during all phase of design, construction, and shakedown. For these projects, the FSSA shall be an integral part of the design process as outlines in Section 3.4.4, “Change Controlled by Design Review Process.” At the start of any new project, the PM or FSH shall contact the SFAB FSSE, who shall initiate the FSSA.

2.3 SOP’S and Checklists

2.3.1 Instructions for the development of SOP’s 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 SOP’s and/or Checklists.

2.4 SOP ~~Guidelines~~[JSP4]Development Requirements

2.4.1 SOP’s are detailed, written, formal instructions for qualified operators to use during operation of the facility. The ~~basic guidelines~~requirements to be followed in the preparation of SOP’s are listed below.

a. SOP’s 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. SOP’s shall be developed in accordance with Appendix D, Requirements for Developing SOP’s/Checklists.
~~a.~~

~~1) SOP's shall be designed to alert operators of potentially unexpected events. These alerts shall be expressed in three distinct categories:~~

~~2) **NOTES.** General instruction to the operator concerning the specific order that procedures must follow. They alert the operator to potential undesired events of a minor nature (that is, failure to comply would invalidate previous actions), and they provide explanatory information.~~

~~3) **CAUTIONS.** Specific alerts to the operator that the sequence, which follows, could cause equipment damage if not executed as specified.~~

~~4) WARNINGS. Specific alerts to the operator that the sequence, which follows, could cause personnel injury or death if not executed as specified.~~

~~b.~~c. SOP's for the complete cycle shall be demonstrated and approved prior to being included in the CM Program.

~~c.~~d. Initially, demonstrations shall be "dry runs" to avoid unnecessary exposure to hazards.

~~d.~~e. SOP's shall be approved by the preparer, reviewer, Safety Manager and FSH.

~~e.~~f. SOP's shall be placed under configuration control in accordance with the requirements of Chapter 3.

2.4.2 Checklist ~~Guidelines~~Development Requirements

a. ~~a.~~ Checklists are abbreviated versions of SOP's and are intended to provide less-detailed instructions for routine, day-to-day operation of a facility by experienced personnel. 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.

b. Checklists shall be developed in accordance with Appendix D, Requirements for Developing SOP's/Checklists.

c. Checklists may cover an entire cycle of operation or any part thereof; however, it shall be clearly labeled as to what it covers.

d. Checklists may be of a "check off" or "sign off" nature, or it may be simply a sequential listing of steps to be taken without the need to check/sign items off.

e. 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.

~~. The developmental process shall be identical to that followed in the development and approval of SOP's. Some guidelines to be used in their preparation are listed below.~~

~~1) A Checklist may cover an entire cycle of operation or any part thereof; however, it must be clearly labeled as to what it covers.~~

~~2) A Checklist may be of a "check off" or "sign off" nature, or it may be simply a sequential listing of steps to be taken without the need to check/sign items off.~~

~~3) A Checklist is often reproduced within the facility and a copy used for each operational run. In such cases, the entire Checklist must be reproduced and no part of the original omitted.~~

2.4.3 SOP/Checklist Organization

a. SOP's/Checklists will be divided into ~~two~~ three sections: Introductory Matter ~~and~~ , Text, and Emergency Procedures.

2.4.3.1 Introductory Matter

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

b. The **Title Page** contains the SOP/Checklist title, the name of the facility for which the document was completed, the facility number in which the facility is housed and the statement **"THIS DOCUMENT CONTAINS HAZARDOUS OPERATIONS PROCEDURES"**.

c. The **Revision Record** reflects all SOP/Checklist document changes as well as who prepared, reviewed, and accepted those changes. These shall be:

1) The "Prepared By" column shall be signed by the person who prepared the change.
2) The "Reviewed By" column shall be signed by the designated reviewing authority.
3) The "Reviewed By~~"~~ Safety Manager" column shall be signed by the Safety Manager or designee.
4) The "FSH Cognizance" column shall be signed by the FSH.

e. ~~d.~~ A **General Introduction** page addresses the purpose, personnel, equipment, support and safety services, ~~equipment,~~ initial conditions, ~~and~~ references, remarks ~~drawings~~ 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, Security, etc.).
5) INITIAL CONDITIONS- A description of assumptions made prior to beginning the tasks/subtask(s), for example, 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).

f. The **Safety Information** section contains information regarding any condition, event, operation, process, or item of 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 shall contain the following:

1) HAZARDS – A statement for the operator(s) to see Facility Resume and SAR for potential conditions that may be hazardous to personnel executing the procedure or to government property. Occupational hazards that are not listed in the facility SAR shall be listed here.
2) COUNTERMEASURES – A statement for the operator(s) to see Facility Resume and SAR for a list safety devices, interlocks, etc. that are employed to reduce the risk to personnel or equipment from the hazards specified above.
3) HAZARDOUS MATERIAL(S) - A statement for the operator(s) to see Facility Resume, SAR, Material Data Sheet Book or log into the Chemical Tracking System Log for a list of hazardous materials that may be encounter during to execution of this procedure.
4) PERSONAL PROTECTIVE EQUIPMENT – List the personnel protective equipment (PPE) required to safely and effectively accomplish the procedure.

2.4.3.2 Text

a. The Text section begins immediately following the Introductory Matter and consists of a Sequence Flow Chart, which shows the safe order in which the preoperational (PR), operational (OP), and post operational (PO) procedures can be executed, followed by the actual, step-by-step SOP/checklist.

2.4.3.3Emergency Procedures

a. The Emergency Procedures section shall specify operator actions to be taken during plant emergencies. Emergency contact information, routes of exit, fire alarms and extinguishers…etc. 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. 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 SOP's/Checklists developed before LPR Effective Date~~Changes and Distribution~~

a. ~~Since~~ SOP's/Checklists developed before the effective date of this LPR~~are CCD's, they~~, ~~-~~requiring only an administrative change, shall not be required to be updated in accordance with the requirements set forth in this document.~~be changed and distributed in accordance with the requirements set fourth in Chapter 3 of this document.~~

2.4.5 SOP's/Checklists Changes and Distribution

a. Since SOP's/Checklists are CCD's, they shall be changed and distributed in accordance with the requirements set forth in Chapter 3 of this document.

2.5 SAFETY ANALYSIS REPORTS (SAR's)

a. A SAR is the formal documentation of the FSSA and shall be prepared in accordance with Section 2.5.2~~Section 2.4.2~~. It shall be a CCD document and any change to the facility will be considered for possible SAR impact.

2.5.1 SAR Organization

a. 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 (for example, a Critical Items List (CIL)) 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.

2.5.1.1 Introductory Matter

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

b. The **Title Page** contains the report title, the name of the facility for which the report was completed, the building number in which the facility is housed, and the Effort Code (EC) associated with the facility.

c. The **Revision Record** reflects all changes to a SAR; who prepared, reviewed, and accepted the report/changes; and the date issued. The required signatures are as follows:

1) The "Prepared By" column shall be signed by the FSSE who prepared the report/change.
2) The "Reviewed By" column shall be signed by the designated reviewing authority.
3) The "Reviewed By Safety Manager" column shall be signed by the Safety Manager or designee.
4) "FSH Cognizance" column shall be signed by the FSH.

d. The **Table of Contents** lists the major subsections of the SAR and the page number on which each begins.

2.5.1.2 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 & Recommendations and Tabular Summary. General Observations and Recommendations address the h~~H~~azards that are general in scope as opposed to specific to a particular subsystem and documents any other fact the FSSE feels is relevant to the SAR but does not belong in an Appendix. The Tabular Summary subsection lists and discusses the identified u~~U~~ndesired e~~E~~vents and the associated risks. The Tabular Summary presents a synopsis of the s~~S~~afety ~~Analysis~~ 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.~~4~~5.4.

2.5.1.3 Appendices

a. 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.

2.5.1.4 Critical Items List (CIL)

a. The SAR includes a Critical Items List (CIL) for any facility that has a Critical Item. A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment/property equal to or greater than $1.0M. Section 2.5~~4~~.2 provides more details about preparing a CIL.

2.5.1.5 SAR Changes and Distribution

a. Since SAR's are CCD's, they shall be changed and distributed in accordance with the requirements set forth in Chapter 3 of this document.

2.5.2 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. Any SAR prepared by a support contractor shall be reviewed and approved by the SFAB FSSE.

b. The following definitions provide a uniform understanding of the terms related to SAR preparation:

1) **Hazard.** A condition which has the potential to result in damage to equipment and/or personnel injury/death.
2) **Undesired Event.** An event (or series of events) which unleashes the potential inherent in a hazard, and either directly or indirectly results in equipment damage and/or personnel injury/death.
3) **Cause.** The stimulus or triggering mechanism/act which precipitates the Undesired Event.
4) **Effect.** The consequence of the Undesired Event in terms of equipment damage and/or personnel injury/death.

2.5.2.1 Phases

a. The phases of SAR preparation is 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. Examples of such subsystems are high pressure air, vacuum, model injection, cooling water, test section, nitrogen, hydrogen, and so forth. How these subsystems are identified in any given facility depends 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.

c. Next, the FSSE performs a **Preliminary Hazard Analysis (PHA)** to identify all the possible Hazards and the 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 will be sent to the Facility Team for initial review and clarification of the facility Hazards and Undesired Events.

d. 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.

e. 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. Details of how to perform a HA are provided in Section 2.54.3.

f. With the subsystems, Hazards, and Undesired Events defined, the FSSE prepares a **Critical Items List (CIL)**, if required. A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment/property equal to or greater than $1.0M. A Critical Item must 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. The requirement for design calculations can be waived for Critical Items which are proprietary or part of a company's standard product line providing that the item has been designed to industry consensus codes, a history of acceptable operations of the same or similar products is available, and the use is in compliance with the manufacturer's ratings and recommended applications. Examples of proprietary items that meet the design waiver criteria are large rotating machinery for wind-tunnel compressor or drive systems. Critical Items listed in a SAR shall be tracked throughout their lifetime for compliance with design, maintenance, and inspection requirements. Pressure components that are standard product lines and built to national consensus codes or standards are not considered Critical Items. However, these items are covered under LaRC's Pressure System Recertification Program to assure system integrity.

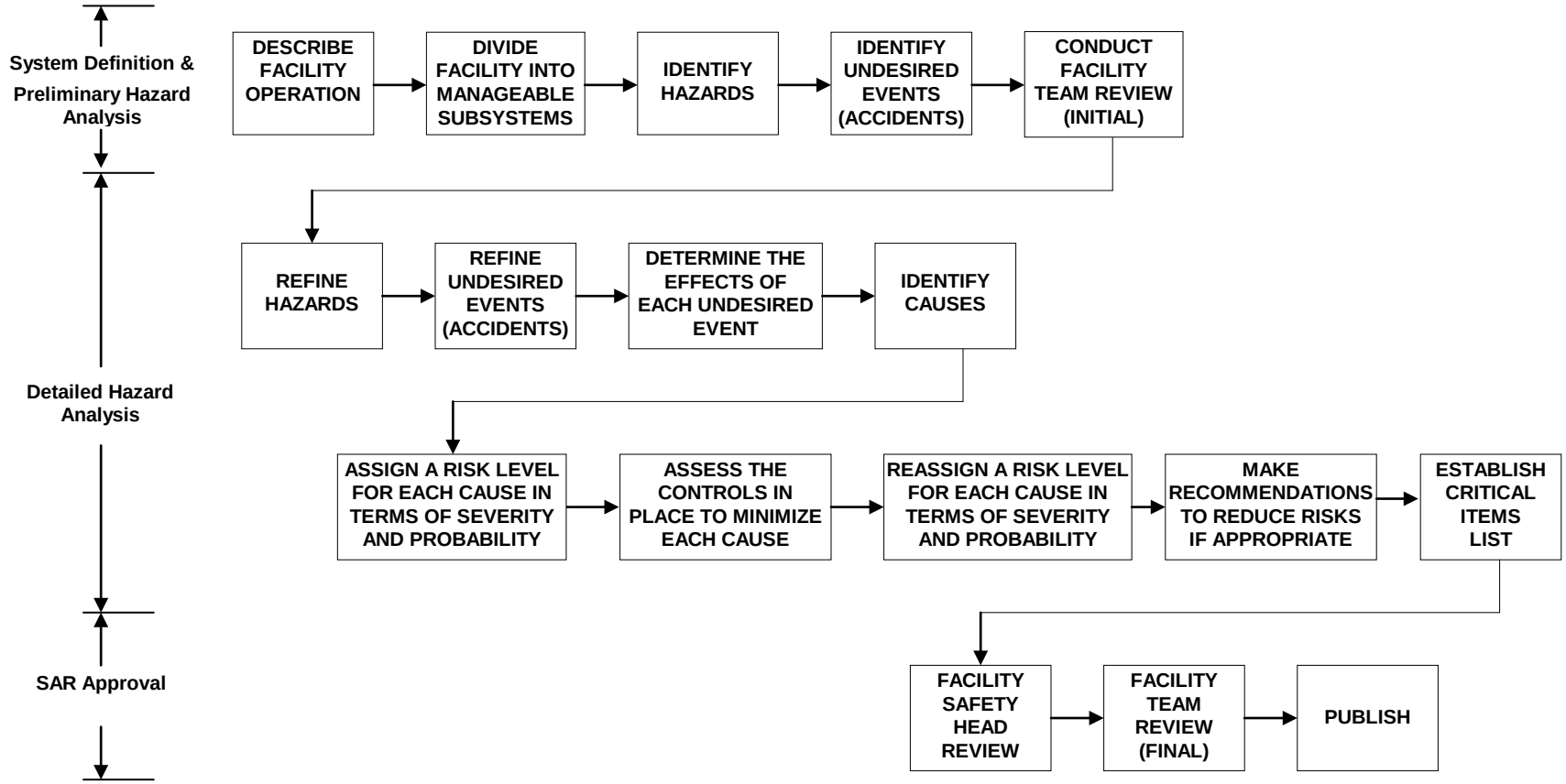

Figure 2-1, SAR Preparation Sequence.

g. 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.

h. 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.

i. 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. Finally, it shall be incorporated into the CM Program.

2.5.3 Hazard Analysis

a. The HA begins with a detailed exploration of each of the identified Hazards (an example of one might be hot surfaces). Considering that Hazard, the FSSE establishes what event(s) could occur that would result in the Hazard causing damage, injury, and/or death (for example, personnel in contact with hot surfaces). Those events become the Undesired Events. There could be multiple Undesired Events resulting from each identified Hazard. The analyst then quantifies the Effects of each Undesired Event in terms of damage, injury, and/or death (for example, serious injury to personnel). When numerous effects result, only the most severe is noted.

b. Next, the FSSE establishes what could cause an Undesired Event to occur, and these become the Causes (for example, personnel error). There could be one or multiple causes for the same Undesired Event. 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. A Risk Assessment Code (RAC) is assigned to each of the identified Causes using the guidance provided in Section 2.54.4. 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.

c. In the interest of plausibility, the Undesired Events, Causes, and Effects are to be confined to “credible" as opposed to “conceivable" events. They should reflect only those things that could reasonably be expected to occur.

d. After the SFAB FSSE has assessed the current hazard controls, the RAC is re-evaluated using the guidance provided in Section 2.~~4~~5.4. If an assigned RAC is unacceptable, as outlined in Section 2.~~4~~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.

HAZARD SEVERITY

The 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 being 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 loss 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 quantitative, 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.

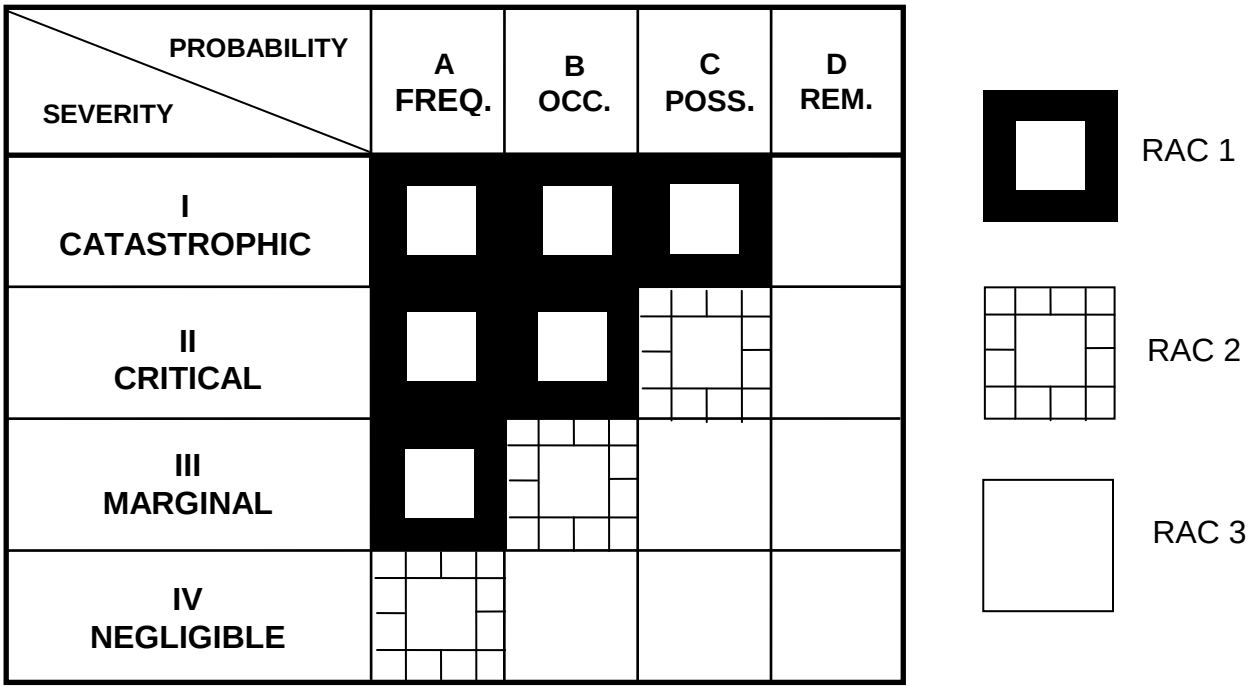

Figure 2-2, Risk Assessment Matrix.

2.5.4 Risk Assessment

a. An alphanumeric risk level, based on both Severity and Probability of Occurrence, shall be assigned to each Cause, before and after hazard controls are in-place, of an Undesired Event. 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."

2.5.4.1 Severity Category

a. A Severity shall be assigned to each Undesired Event assuming it will occur. In this analysis, the worst possible results is to be assumed with no consideration being given to abatement techniques incorporated in the system design or to the use of procedures. The Severity Category provides a relative measure of the worst possible consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, and subsystem or component failure/malfunction. The Severity Categories are:

1) **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.
2) **Category II - Critical** - May cause lost time injury or illness, and/or system/equipment damage between $250,000 and $1,000,000.
3) **Category III - Marginal** - May cause minor injury or illness, and/or system/equipment damage between $1,000 and $250,000.
4) **Category IV - Negligible** - Will not result in injury, illness, or system/equipment damage not in excess of $1,000.

[JSP5]2.5.4.2 [JSP6]Probability of Occurrence Level

a. A Probability of Occurrence shall be assigned to each Cause, before and after hazard controls are in-place, of an Undesired Event. The Probability of Occurrence provides a measure of system safety by evaluating the system design in conjunction with abatement techniques, inspections, tests, and operating procedures. The Probability of Occurrence is the probability that a failure will occur sometime during the planned life of the system. The probability level shall be qualitatively based upon engineering judgment with appropriate guidelines. Those guidelines are:

1) **Level A - Frequent** - The level assigned when neither a safety feature nor approved procedures exist to prevent the Undesired Event from occurring.
2) **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.
3) **Level C - Possible** - The level assigned when approved procedures do not exist, but an existing safety feature should prevent the Undesired Event from occurring.

4) **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.

2.5.4.2 Establishing a Risk Assessment Code (RAC)

a. First, the Effect of an Undesired Event is evaluated in terms of Severity (I, II, III, or IV). 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 (for example, IA, IIB, IIIC, etc.). Finally, using the two-dimensional risk matrix, Figure 2-2, each risk level is translated into one of three Risk Assessment Codes (RAC's) - RAC 1, RAC 2, or RAC 3. They are pattern-coded on the matrix to distinguish each from the other. RAC 1's include blocks IA, IB, IC, IIA, IIB, and IIIA. RAC 2's include blocks IIC, IIIB, and IVA. All other blocks are RAC 3's. After the in-place hazard controls are assessed, the above assessment is repeated using the newly established probability of occurrence.

2.5.4.3 Implications of a Given RAC

a. A RAC is a measure of the severity of an Undesired Event verses 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 1's** 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 1's for new facilities, and those associated with a major Construction of Facilities (CoF) project in an existing facility, are of major 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 1's 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: (1) resolution (i.e., reduction of the RAC from 1 to a 2 or 3), (2) an abatement plan approved by the Safety Manager, or (3) approval by the Executive Safety Council (ESC) before the facility can resume operation. Failure to meet one of these requirements could result in facility shutdown.

c. **RAC 2's** 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 2's for new facilities and those associated with a major CoF in existing facilities are also of concern and require special attention. The FSH of the facility in question, with Safety Manager concurrence, shall by letter, inform the Organizational Unit Manager who oversees the facility of the nature of the RAC 2 and request approval to conduct operations. Operations shall not begin in that facility until the Organizational Unit Manager, with the concurrence of the Safety Manager and Chairperson of the final design review board has responded by letter authorizing such action.
2) **Existing** - RAC 2's for existing facilities not undergoing a major CoF require no such approval. Acceptance of the risk is acknowledged by the SFAB FSSE, Safety Manager, and FSH by signing the SAR. Plans and programs to correct existing RAC 2 UE's, as time and resources permit, are considered sound management practice.

d. **RAC 3's** are at a risk level that only needs to be accepted 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

a. In order to conduct 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.

1) A credible single order failure that can jeopardize personnel or major equipment requires an interlock or protective device to prevent its occurrence.
2) 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.
3) 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 (for example, hardwired backup of a software safety interlock or device).
4) 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.

5) 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 of this handbook. At no time shall software changes be made while the facility is on line (in operation).
6) Forcing of 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.
7) Failures of catastrophic proportions identified by the FSSA shall be assessed individually in the safety analysis and redundant safety interlocks or devices provided.

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

2.6.1 Design

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

2.6.2 Engineered Safety Features

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

2.6.3 Safety Devices / Personal Protective Equipment

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

2.6.4 Warning Devices

a. 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.

2.6.5 Procedures/Training

a. 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). The process shall be controlled by SOP’s. 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 DRAWINGS AS CCD’s

a. 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 Configuration Control Documentation (CCD) and placing these documents in the Facility CM Program. CCD documents will include the SAR, the SOP’s 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 drawing that:

1) Supports the conclusions of the safety analysis, and/or
2) Useful for troubleshooting electrical systems,

~~b.~~ are designated as CCD.

b. Members of the Facility Team may include other drawings as CCD, if desired.

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

Chapter 3

3. FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM

3.1 PROGRAM SUMMARY

a. The LaRC Facility CM Program includes the facilities in Figure 1-1, "Effort Code Summary." LaRC's CM Program provides for the ability to:

1) Record and maintain safety analysis documentation,
2) Document and maintain standard operating procedures (SOP's) for use by operating personnel,
3) Ensure the Safety and Facility Assurance Branch (SFAB) reviews changes that affect safety, and
4) Establish and maintain a baseline for designated systems (e.g., electrical systems) and the relevant configuration control documentation (e.g., drawings).

b. In addition, the Facility CM Program provides for risk reviews that consist of Annual CM Meetings[JSP7], Procedure Demonstrations, and continual Facility System Safety Engineering Analyses.

3.2 CHANGE CONTROL

a. 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 SOP's shall be processed through the CNS process. 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.

b. The CNS process requires the Facility Coordinator (FC), the Facility Safety Head (FSH), the Facilities Configuration Coordinator (FCC), and the Safety Manager, or designee, to approve a CNS prior to any hardware changes.[JSP8] 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. SAR's, SOP's, checklists, drawings, etc.) are redlined prior to implementation of the change.

c. The CNS process shall be conducted in accordance with one of two Langley Management System (LMS) Center Procedures (CP) - LMS-CP-4710, “Configuration Management for Facilities” and LMS-CP-4890, “Construction and Change Assurance for High Risk Facilities.” 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.

3.3 UPDATING AND DISTRIBUTING CCD

a. All CCD’s shall be updated in accordance with the redlined documents submitted through an approved CNS. Updating CCD’s shall not occur until after the changes proposed by the CNS have been completed. All updated CCD’s shall be distributed as outlined in this section.

b. For each CNS completed, a distribution package will be generated. The package includes a cover letter that includes the statement "this is a completion of CM update and delivery CCD revision package" and includes at least the following information: CNS Number, EC, Facility Name and Building ~~n~~Number. Each updated CCD shall be included as enclosures to the package. The FSH shall receive a package that includes the enclosures marked "Working Master”. A cover letter without enclosures shall be sent to the FC and Safety Manager, or designee.

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 required 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

a. 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. A CNS shall be required to update Pressure Systems Documents (PSD's) when like for like replacements are made in a high-pressure system, and the CNS process shall be conducted in accordance with LMS-CP-4710.

3.4.2 No Safety Impact

a. 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.

3.4.3 Safety Impact

a. 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. There are two possible "paths" through this process. The path chosen depends if the change is being conducted in accordance with LAPD 7000.2, "Review Program for Langley Research Center (LaRC) Facility Projects," or not. Changes that are governed by LAPD 7000.2 are conducted as outlined in Section 3.4.4.

b. For changes that are not governed by LAPD 7000.2, a CNS shall be initiated and submitted through the CMOL system. 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. Prior to the Safety Manager's approval, the SFAB FSSE responsible for the facility shall conduct a safety analysis. After approval by the Safety Manager, or designee, the package shall be forwarded to the FCC for approval. 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

a. 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.

1) 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.
2) 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.
3) Following the PDR, the SFAB FSSE 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 CCD's.
4) 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 assure all CCD drawings are field verified prior to the Integrated System Review (ISR).
5) At the ISR, the FSSE shall attest that all drawings previously identified as CCD's have been FV and present the results of the safety analysis.
6) At the Operational Readiness Review (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.
7) 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

a. This section describes several unique aspects of drawings incorporated into the CM Program and designated as CCD. Section 2.7~~6~~ provides guidelines for which drawings should be placed under configuration control.

3.5.1 Drawing Field Verification

a. All engineering drawings currently in the CM Program shall be classified as either field verified (FV) or unverified. Additionally, no new drawing shall be brought into the CM program (i.e., designated as CCD) unless it is first FV.

b. The field verification process shall be a hands-on verification of the validity of the drawing conducted by facility, SFAB, Project and Engineering Branch (PEB), or contractor personnel. A drawing which has been FV shall display a "FIELD VERIFIED" statement authenticating that action. That statement shall be signed by the person attesting to the field verification. It shall also be signed and dated as approved by the Project Manager (PM), FSH, or FC. If FV drawings are found

discrepant, they shall lose their FV status and shall be identified as unverified. A sample of the FV statement is as shown below.

FACILITY BASELINE DRAWING
FIELD VERIFIED BY: _____
APPROVED BY: _____
LATEST DATE: _____

c. 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.

WARNING!
UNVERIFIED

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

3.5.2 **Changes to CCD Drawings**

a. When drawings in the CM Program require change, the drawing shall be redlined. New items are added in green ink or in black ink highlighted in yellow marker. Existing items are deleted by marking over them in red ink. Redlined drawings shall be processed using the CNS process. 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

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

b. In those cases where there are a number of CCD drawings which 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. In addition, each of the affected facilities shall receive a new drawing marked WORKING MASTER in red ink. 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. 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.

c. Adherence to the following additional guidelines promotes accountability and use of WORKING MASTER drawings:
   1) A WORKING MASTER drawing shall always reflect the true ("as-built") configuration of the facility, which it represents.
   2) 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.
   3) Changes, which reflect “as-built” configurations, shall be marked on the WORKING MASTER of each affected CCD drawing.
   4) 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

a. A Facility Baseline List (FBL) can be generated for each facility in the CM Program using Configuration Management On-line (CMOL). The FBL represents a list of all CCD documents for the Facility. For those facilities that choose, a list of Supporting Facility Documents (SFD’s) will be maintained on CMOL. SFD’s 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 CCD’s, 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 CCD’s

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

3.7.1 Engineering Drawing Files (EDF)

a. EDF shall be the repository for all original (reproducible) configuration controlled drawings and for the electronic historical records of configuration controlled drawings and other CCD’s. EDF will preserve these historical records and all subsequent changes. Only a Configuration Management Engineer, with the Configuration Management contractor maintaining CMOL, shall be permitted to

withdraw CCD original drawings from EDF. Analyses, drawings, and nondestructive engineering information for systems that have been recertified or identified in the CIL shall also be stored in EDF.

3.7.2 Facility Files

a. Each facility shall maintain its own filing system of current WORKING MASTER CCD's. 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 CM REVIEW

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

~~1.3.1~~ 3.8.1 Annual CM Meetings[MSOffice9]

a. Annual CM Meetings shall be held for each LaRC facility in the CM Program to review facility documents and status, plans, and program effectiveness. These meetings shall be scheduled by the SFAB FSSE. Attendees include the FCC, FSH, FC, SFAB FSSE, and CM Engineer. SFAB FSSE shall issue a letter summarizing the meeting and delineating "action items." The minutes shall be permanently maintained by SFAB FSSE as documentation that the CMOL documents have been reviewed and re-approved.

~~1.3.2~~ [JSP10]3.8.2 [JSP11]Procedure Demonstrations[MSOffice12]

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

1) Facility Safety Head
2) LaRC Safety Manager, or designee
3) CM Engineer
4) Certified Operator(s)

b. Procedures which have not been verified or used within the last 12 months, shall be verified by a Procedure Demonstration. At the completion of a Procedure Demonstration, the CM engineer shall notify all participants which procedures were demonstrated and the CNS numbers associated with any required changes.

~~1.3.3~~ 3.8.3 Continual Facility System Safety Engineering Analyses

a. 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. SAR's, SOP's, Checklists, and engineering drawings) are analyzed to assess the safety impact of the proposed changes.

3.9 CONFIGURATION MANAGEMENT ON-LINE (CMOL)

a. CCD's 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 CCD's and provides for electronic CNS processing (i.e., CNS Workflow).

~~1.3.4~~ [JSP13]3.9.1 Access and Database Maintenance

a. Access to CMOL shall be by authorized personnel at "https://cmol.ndc.nasa.gov/~~https://cmol~~." Entry into the CMOL system shall be controlled by use of an employee's Agency User ID (AUID) and associated password. [JSP14]~~Access to CMOL may be obtained by following the instructions at http://lms.larc.nasa.gov/cmol_documents.cfm~~. SFAB shall approve any request for an account that requires authority to approve a CNS.

[JSP15]

b. New documents shall be entered into the CMOL database within 10 working days of final approval[JSP16][JSP17]. If there is a question concerning the currency of a particular document, contact a representative from SFAB for assistance and/or confirmation.

~~1.3.5~~ 3.9.2 CNS Initiation/Processing

a. 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 allows for three options from which to select. 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. The third option allows the user to view the status of CNS Work Packages over which the user has authority or requires the user's attention (i.e., review and approval).

Chapter 4

4. PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM)

4.1 PROGRAM SUMMARY

a. As part of LaRC's Pressure Systems Recertification Program, a Pressure Systems Document (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 Maintenance of Ground-Based Pressure Vessels and Pressurized 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.

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

c. 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 (PSD)

a. 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 Maintenance of Ground-Based Pressure Vessels and Pressurized Systems." The PSD is a compendium of component information and sketches and consists of:

1) **Title Page** - Identifies the document as a PSD, the facility number and name, the system name and designation, and the PSCM document number.
2) **PSCM Revision Record** – Reflects the approval of all issues of the PSCM.
3) **Table of Contents**.
4) **Introduction** - Discusses the development, purpose, and uses of PSCM.
5) **Definition of Symbols**.
6) **Key to Recertification Sheets** (Component Inventories).
7) **System Description**.
8) **Isometric Drawings**.
9) **Recertification Status Sheets**.
9)
10) **Footnotes**.
11) **Document Reference Sheet**.

Chapter 5

5. FACILITY SOFTWARE ASSURANCE AND CONFIGURATION MANAGEMENT

5.1 GENERAL

a. The use of automated control systems, for example programmable logic controllers (PLC) and PC's, by LaRC research facilities has generated the need for configuration control of software, including PLC logic. This chapter outlines the requirements for the Software Configuration Management (SCM) Program at LaRC research facilities.

5.2 PROGRAM OVERVIEW

a. The development/acquisition of software products for LaRC research facilities shall be in accordance with LMS-CP-5528, "Software Planning, Development, Acquisition, Maintenance, and Operation." The required level of configuration control during development shall be in accordance with LMS-CP-5528 and meet the requirements of LMS-CP-5529, "Software Configuration Management Planning for Low-, High-, and Critical-Control Software."

b. Each research facility using an automated control system that is responsible for performing safety functions (e.g., correct valve sequencing, shutdown the facility in an over temperature condition) shall develop a Software Configuration Management Plan (SCMP). Programmable logic controller (PLC) logic is considered software for facilities that use a PLC to control facility systems and/or perform safety functions.

c. The SCMP shall be developed in accordance with LMS-CP-5529, and placed under configuration control in CMOL. In addition, the plan shall define a process to identify and review changes that directly affect safety prior to implementation. Changes that modify a hazard control (e.g., interlocks, valve sequencing) of an Undesired Event identified in the Safety Analysis Report (SAR) or affect the safety of the facility shall be processed using a Change Notification Sheet (CNS). This ensures a safety review by the FSH, the FC, a SFAB FSSE, and a PEB representative. The CNS also ensures other CCD documents (e.g., SAR) are updated as required. The Software Configuration Manager (SCM), who shall be defined in the SCMP, shall initiate the CNS. If the SCM has any question about the safety impact of a change, the FSH or an SFAB FSSE shall be consulted.

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

Chapter 6

6. LANGLEY RISK EVALUATION PROGRAM (LREP)

6.1 PROGRAM SUMMARY

a. The Langley Risk Evaluation Program (LREP) has been established to provide a systematic review of the energy sources utilized by research equipment and operations at LaRC. This review mechanism allows SFAB to identify any potential hazards associated with the~~i~~se 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 shall be reviewed by SFAB for inclusion into LREP before the equipment is purchased and installed on Center.

Equipment/Operations Required for Review		
Electrical • Permanently installed, operating at or above 50 VAC/VDC. Example: Wind-tunnel motor, 240-volt, 3-Phase.	**Thermal** • External surfaces in excess of 130 °F. • Internal temperatures in excess of 212°F. • Utilizing cryogenic fluids Example: Vacuum Furnace, Operates internally to 3000°F	**Pressure** • All pressurized/vacuum systems Example: MTS test stand, hydraulic pressure at 3000psi
Human Interactions • Requires the use of an external piece of equipment (e.g. – laptop, pendant) to operate. Example: MTS test stand with personal computer workstation; provides main user-interface.	**Chemical Reactions** • Utilized to initiate chemical reactions or a byproduct of operations Example: Plasma flow control apparatus, generates ozone and other pollutants as a byproduct	

Figure 6-1, Equipment/Operations LREP Energy Source Levels.

b. ~~Equipment~~ Facilities identified with an FRI of ~~MODERATE~~ 2 shall be included in the LREP program, (see Appendix C2.2 for more information) and any other ~~facility~~ system which has been determined by SFAB to be included in LREP.

c. Equipment/Operations held under the former Laboratory Risk Evaluation Program will be historically archived, unless the equipment/operations are still viable and will be evaluated under this Chapter.

d. The elements associated with the LREP program are a Langley Risk Evaluation and a Job Hazard Analysis. These documents shall be maintained in the Facility Resume.

6.2 LANGLEY RISK EVALUATIONS (LRE's)

a. The term Langley Risk Evaluation (LRE) was established to identify the Safety Analysis efforts associated with the LREP. A 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 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.

b. A LRE consists of a Title Page, Revision Record, and a series of tables: Identification of Equipment, Energy Source (s), Hazard Controls, Identified Job Hazard Analysis, and General Observations/Recommendations. Below each section is described in further detail.

1) **Title Page** – Identifies the document as an LREP product, states the name of the equipment, and provides the facility number in which the equipment is located.
2) **LREP Revision Record** – Reflects the approval signatures for the initial issue and all LRE changes.
3) **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 operators required to utilize the equipment.
4) **Energy Source (s) –** All the energy sources associated with the operation of the equipment are identified ~~technically~~ (e.g. – for Electrical, state the voltage and amps used by the equipment; for Pressure, state the medium and pressure).
5) **Energy Controls –** Provides for the identification and location of all controls which will isolate the energy from the equipment and bring the equipment into a dormant state.
6) **Job Hazard Analysis –** Identifies the associated JHAs, which have been developed in accordance with LPR 8717.1, which are used by the operators while operating the equipment
7) **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 (i.e. noise levels, power demands, effects of equipment malfunction, etc.). Establishes recommendations, if any identified new/existing conditions present unacceptable risk to personnel or equipment.

~~6.3~~ LREP CHANGES AND DISTRIBUTION

a. LREPs shall be reviewed during the annual Facility Resume review by the FSH. If the review determines that changes are necessary to the LREP, the following actions shall be completed:

1) ~~(1)~~ the FSH shall contact the appropriate SFAB FSSE for their facility and notify them of the requested change
2) ~~(2)~~ the SFAB FSSE shall review/approve the proposed changes ~~(~~
3) ~~3)~~ the SFAB FSSE shall revise the LREP.

After the LREP has been revised, the SFAB FSSE shall forward the LREP to the FSH for review/approval. A copy of the ~~The~~ revised LREP shall be ~~placed back~~ kept by SFAB and the original placed into the facility resume.

Chapter 7

7. ASBESTOS CONFIGURATION MANAGEMENT

7.1 PROGRAM SUMMARY

a. The objectives of LaRC's Asbestos Safety and Configuration Management Programs are:

1) Enable LaRC to comply with the myriad of clean air emission regulations established by the Environmental Protection Agency (EPA), the Occupational Safety and Health Administration (OSHA), and the Commonwealth of Virginia;
2) Increase safety awareness and minimize the risk of asbestos exposure to personnel; and
3) Institute controls to prevent the release of asbestos fibers, restrict future asbestos use, and develop surveillance and control of known, existing asbestos applications in LaRC facilities.

b. The safety requirements for asbestos removal are addressed in LPR 1740.2, "Facility Safety Requirements." In summary, prior to any operation involving removal and repair of known asbestos or any other procedure that may release airborne asbestos, an inspection must be performed by an inspection team. The team shall include a SFAB Industrial Hygienist (IH). In addition, operational and control procedures shall be documented, and prior to the start of operations, approved by the SFAB.

c. This chapter addresses the configuration management of known, existing asbestos applications in a facility. Each facility has been inspected to identify friable and nonfriable asbestos containing building material (ACBM) and written inspection reports were provided to the FSH's. These inspection reports were the baseline documents used to generate the Asbestos Configuration Management Reports (ACMR).

7.2 ASBESTOS CONFIGURATION MANAGEMENT REPORTS

a. An ACMR provides facility personnel, especially the FSH and FC, a document that identifies known asbestos applications. The report consists of:

1) **Title Page** – Identifies the document as a configuration controlled document, identifies the facility by number and name, and identifies the current document revision.
2) **Revision Record** – Reflects the approval signatures for the initial issue and all subsequent changes.
3) **List of Page Revisions** – Enumerates each page in the document and the current revision letter of each page.
4) **Introduction** – Provides the purpose and philosophy of the document.
5) **Facility Asbestos Summary** – Describes in narrative form the asbestos status of the facility.
6) **Facility Diagram** – Depicts the actual location of positive samples where asbestos is located in the facility.

7.3 ASBESTOS CM CHANGES[MSOffice18]

a. Upon receipt of Langley Form 27, "NASA LaRC Asbestos Safety Permit", and completion of an Asbestos abatement project, the SFAB Industrial Hygienist [JSP19]shall submit a CNS for revision to the facility ACMR with the completed LF 27 as an attachment to CMOL. The revised ACMR shall be approved through CMOL utilizing LMS-CP-4710.~~submitted to FSH for approval and distributed to the FSH and SFAB Industrial Hygienist..~~

[JSP20]

Appendix A

A. GLOSSARY OF KEY TERMS

Asbestos CM Program (ACMP). A program designed to ensure NASA Langley Research Center (LaRC) compliance with asbestos-related EPA, OSHA, and Commonwealth of Virginia clean air emission regulations. This program generates and maintains current records of the location and status of all known asbestos at the Center.

Cause. The stimulus or triggering mechanism/act which precipitates an Undesired Event (accident).

~~**Change in Laboratory Equipment/Procedures (CLEP) Form.** NASA Langley Form 129 prepared by LaRC personnel and processed by contractor personnel. It is used in the Laboratory Risk Evaluation Program (LREP) to request approval of and record all changes made to the affected LREP equipment/procedures and it's supporting CCD's.~~

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 CCD's.

Checklist. An abbreviated set of written instructions for operating a facility. Checklists are derived from SOP's and contain sufficient detail to enable safe operations by the most experienced operator personnel. Checklists are developed and maintained under the CM Program.

Configuration Controlled Documents (CCD's). Those facility baseline documents that are considered critical to describing how a facility is configured, how it is to be operated, and what risks are associated with its operation. As such, CCD's are revised only through a formal change process under the CM Program. Examples of CCD's include, but are not limited to, Safety Analysis Reports (SAR's), SOP's and Checklists, certain Pressure System Documents (PSD's), and selected engineering drawings.

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.

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 CCD's electronically via their desktop computer.

Critical Items List (CIL). A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment or property equal to or greater than $1.0M. A CIL is a listing of such items for the affected facility.

Effect. The consequence of an Undesired Event/Accident in terms of equipment damage and/or personnel injury/death.

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 CCD's 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 CNS's prior to any CM facility hardware changes which 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 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 CCD's affecting the 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 Team. Personnel assigned to establish and prepare the Configuration Controlled Documents (CCD's) 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 assigned to the System Safety effort, and the Configuration Management (CM) Engineer from CM contractor.

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 which has the potential to result in damage to equipment and/or personnel injury/death.

Job Hazard Analysis (JHA). 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.

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 (LRE;s) and Job Hazard Analysis (JHAs) ~~Langley Operating Procedures (LOP’s)~~ to selected ~~laboratories~~ equipment at LaRC which are not in the CM Program and not covered with a Safety Permit.

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.

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

CM Contractor. The CM Contractor is the Non-personal Services Contractor who supports the LaRC Facility CM Program.

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). A 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 which documents the formal Facility System Safety Analysis of a particular research 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.

Safety Manager, SFAB, SMAO. This individual reviews and approves all System Safety Analyses and reviews all changes to the SAR's, SOP's, 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.

Standard Operating Procedures (SOP's). Detailed, written, step-by-step instructions to be routinely followed in operating a facility. SOP's contain all of the information considered pertinent to safe and efficient operation of the facility. SOP's are the source documents for Operational Checklists and are the basis, in part, for the facility Hazard Control Analysis. SOP's may also be used for training operator personnel. SOP's 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 (SFD's). Those documents identified on the SFD list that are considered as part of the baseline documentation, but do not meet the criteria for CCD's.

Undesired Event. An event (or series of events) which unleashes the potential inherent in a hazard and, either directly or indirectly, results in damage and/or personnel injury/death.

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 personnel injury, unacceptable equipment/facility damage, and/or loss of productivity.

Working Masters. Copies of the latest-revision CCD's (SAR's, SOP's, drawings, and so forth) which are stamped "WORKING MASTER" in red and kept at the facility.

Appendix B

B. ACRONYMS

ACBM	Asbestos Containing Building Material
ACMP	Asbestos Configuration Management Program
ACMR	Asbestos Configuration Management Reports
CCD	Configuration controlled documentation
CDR	Critical Design Review
CIL	Critical Items List
CLEP	Change in Laboratory Equipment/Procedures
CM	Configuration Management
CMOL	Configuration Management On-Line
CNS	Change Notification Sheet
EC	Effort Code
EDF	Engineering drawing files
EPA	Environmental Protection Agency
FBL	Facility Baseline List
FC	Facility Coordinator
FCC	Facilities Configuration Coordinator
FRI	Facility Risk Indicator
FSH	Organizational Facility Safety Head
FSSA	Facility Systems Safety Analysis
FSSE	Facility System Safety Engineer
FV	Field Verified
HA	Detailed Hazard Analysis
ISR	Integrated System Review
JHA	Job Hazard Analysis
LRE	Langley Risk Evaluation
LREP	Langley Risk Evaluation Program
OP	Operational Procedures
ORR	Operational Readiness Review
PEB	Project & Engineering Branch, Center Operations Directorate
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controllers
PO	Post-Operational Procedures
PR	Pre-Operational Procedures
PSCM	Pressure Systems Configuration Management
PSD	Pressure Systems Document
RAC	Risk Assessment Code
SAR	Safety Analysis Report
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCR	Software Change Request
SFD	Supporting Facility Documents
SOP	Standard Operating Procedures

Appendix C

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 for a facility 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 the facility, this assessment will help identify the system safety activities which should be accomplished in order to ensure the safety of public, personnel, and property at LaRC. There are four FRIs ranging from a FRI of ~~"High"~~1 to a FRI of ~~"Very Low"~~ 4. The potential hazards inherent to the facility are evaluated using the following criteria as evaluation factors:

1) Public Safety – hazards which could potentially harm the public in any form or manner.
2) Life Safety - hazards which could potentially cause death or serious injury to personnel.
3) Facilities Protection - failures which could cause serious damage to facilities or equipment resulting in significant financial loss.

C.2 FRI Assessment Classification

a. All LaRC facilities shall be assigned a FRI from ~~"High"~~1 to 4~~"Very Low"~~, based on identified potential hazards present in the facility, and their impact on Public Safety, Life Safety, and Facilities Protection. A FRI shall be given to a new facility prior to the start of research activities in that facility. Also, FRI shall be re-evaluated prior to the start of research activities at an existing facility that has undergone a Construction of Facility (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. The following definitions shall be used to classify LaRC facilities and the suggested safety activities warranted after the assignment of the FRIs. Refer to LMS-OP-8715 for the operational procedure in determining a FRI.

C.2.1 FRI ~~- HIGH~~1 (High Risk)

a. Definition- There is a HIGH risk that identified potential hazards in this facility can cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more persons, an occupational injury or illness resulting in a restricted workday or OSHA recordable incident, a first aid incident, or damage to equipment or property in excess of $1,000,000, or any injury/property damage to public.

b. Suggested Safety Program Requirements:
   1) Placement in the Facility Configuration Management Program.

c. All utility facilities (i.e. – substations, sewage plants, etc.) are classified with a FRI of ~~"High"~~1. Any other ~~facility~~ system which has been determined by SFAB to have an inherent high risk associated with it may also be classified with a FRI of ~~"High"~~1.

C.2.2 FRI ~~– MODERATE~~2 (Moderate Risk)

a. Definition- There is a MODERATE risk that identified potential hazards in this facility can cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more persons, 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~~ system which has been determined by SFAB to have an inherent moderate risk hazard associated with it may also be classified with a FRI of ~~"Moderate"~~2.

C.2.3 FRI ~~– LOW~~3 (Low Risk)

a. Definition- There is a LOW risk that identified potential hazards in this facility can cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more persons, 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 on all hazardous facility operations.
   2) Adherence to applicable codes, standards, and regulations.

c. Any facility which contains some form of a shop (i.e. - machine, pipe fitting, HVAC, etc.) is classified with a FRI of ~~"Low"~~3. Cooling towers at LaRC are considered to have a FRI of ~~"Low"~~3. Any other ~~facility~~ system which has been determined by SFAB to have an inherent low risk hazard associated with it may also be classified with a FRI of ~~"Low"~~3.

C.2.4 FRI ~~– Very Low~~4 (Very Low)

a. Definition- There is a VERY LOW risk that identified potential hazards in this facility can cause loss of life, permanent disability, the hospitalization of three or more people, a lost-time injury to one or more persons, 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. ~~c.~~ Any facility which is solely used for office space is classified with a FRI of ~~"Very Low"~~4. All vacated and abandoned facilities are classified with a FRI of ~~"Very Low"~~4. Any other ~~facility~~ system which has been determined by SFAB to have an inherent very low risk hazard associated with it may also be classified with a FRI of ~~"Very Low"~~4.

Appendix D

D. REQUIREMENTS FOR DEVELOPING SOP'S/CHECKLISTS

1.0 INTRODUCTION

The purpose of this Instruction is to establish the procedures for the development, implementation, and revision of Standard Operating Procedures (SOP's) in a standardized format.

This instruction establishes the requirements for developing, implementing, and updating SOP's into a standard format. With NASA LaRC facility/ system operators frequently being Qualified Operators of several different facilities/ systems, standard format SOP's are desirable in an effort to decrease the potential of an accident or incident due to operator error.

This instruction should be closely followed when developing SOP for new facilities. Deviations from this instruction may be permitted to enhance clarity but must be approved by the Facility Safety Head (FSH), the Facility Coordinator (FC), the Operators, and the Safety and Facility Assurance Branch (SFAB).

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 for operators and may increase rather than decrease risk associated with facility operations.

2.0 GENERAL

For the purpose of this instruction, SOP's are defined as detailed, written, formal instructions for qualified operators to use during operation of the facility. SOP's 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.

2.1. 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) may describe the assumed 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 SOP's where equipment is normally left in the position needed for operation. The equipment list(s) may also provide(s) 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.

2.2. 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.

2.3. POST-OPERATIONAL

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

2.4. TASK AND/ OR SUB- TASKS

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 that tasks must be performed, at the facility safety head's discretion.

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 one 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.

2.5. 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 describes, will afford safe and reliable operation. The steps are to be presented in a chronological order and will be sufficiently detailed to permit a qualified operator (per LPR 1740.7) to safely operate the facility/ system.

3.0 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 team will discuss the

Sequential Flow Chart with the operators of the facility/system to ensure proper flow. A single task procedure does not require a flow chart.

4.0 STANDARDIZATION

4.1. TASK IDENTIFICATION

Each Task or Sub-Task shall have an identification designation. An example of an identification designation for a Task or Sub-Task in a set of SOP's is 22-PR-1-A. Each of the parts of the identification designation is defined below.

(1) 22- Identifies the facility/ system by EC number. This number is assigned by CM Program and is currently from 01 to 100.

(2) PR- Identifies the task as a Pre- Operational Procedure (PR), an Operational Procedure (OP) or a Post- Operational Procedure (PO). Other supporting procedures utilized at the National Transonic Facility (NTF) shall use the existing designations, namely: MOP (Maintenance Operating Procedure), MIP (Maintenance Instruction Procedure), IOP (Integrated Operating Procedure) , PMP (Preventative Maintenance Procedure), SEP (Safety and Emergency Procedure), AIP (Alarm/Alarm/Response Policy), and IDSP (Instrumentation and Data System Procedure).

(3) 1 – Identifies the sequential flow task(s) of the SOP task and may be omitted if there is only one task. Generally, series listed must be done 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 done in every run condition and require the operator to determine which tasks need to be performed for the particular run.

(4) 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 (A, B, etc.) 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.

4.2 PAGE IDENTIFICATION

(1) The Task Identification shall be entered in the upper right hand corner of each page.

(2) Page numbers shall be entered at the bottom center of each page.

(3) Revision identification shall be entered in the bottom right hand corner, Rev. A, etc.

(4) The statement, “Configuration Controlled Document”, shall be entered at the top center of each page. Page number shall be bottom centered followed by revision right justified. A mandatory statement concerning requirement for use shall be at the bottom of the page.

4.3 STEP FORMAT

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

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

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

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

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

(5) The equipment commanded will identify the switch, light, push-button, circuit breaker, disconnect switch, etc. 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.

(6) The final state and/ or reaction of the equipment will be stated in capital letters. Examples of final states and/ or reactions are ILLUMINATED, EXTINGUISHED, CLOSED, OPEN, etc. 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. Example, “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. Example, "Clear the test chambers of all personnel, close the test chamber door, and secure all dogs on the test chamber door."

(7) The color of a light, switch, etc. will have the first letter capitalized only. Example: Green, Red, Clear, etc.

(8) In unique situations when step clarity is enhanced, the Safety Office may approve deviations from (a) through (d).

4.4 NOTES, CAUTIONS, AND WARNINGS

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

(1) NOTES may be used when all sequences in the steps cannot be clearly defined.

(2) A NOTE is a step delineator; it is not a step replacement.

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

(4) A NOTE may be used to identify the location where step (s) is performed.

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

(6) A NOTE may precede a step that requires specific instructions.

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

(8) A NOTE will be enclosed in a manner as shown below.

Note: An operating procedure, technique, etc., which requires special emphasis for successful completion of the task

(9) A CAUTION statement will precede any step or series of steps that if performed improperly, as defined in the hazard control analysis, could damage equipment. A CAUTION statement shall be written in bold-face as shown below:

CAUTION

A caution will be accented in this manner.

(10) A WARNING statement will precede any step or series of steps that if performed improperly, as defined in the hazard control analysis, will

endanger personnel. A WARNING statement will be enclosed as shown below:

WARNING
Do not touch the exposed electrical terminals. The electrical terminals are at mains voltage. Touching the electrical terminals may result in death or serious injury.

4.5 CHECKLISTS

A checklist is a shortened form of the SOP's and is used by operations personnel to run the facility/ system on a daily basis. The need for a checklist is a joint decision between the FSH, FC, and the Safety Office. A checklist is not required for all facilities/systems, HOWEVER, if a checklist exists in the SOP's, it must be CCD and used every time the facility/ system is operated.

The length of a checklist is left to engineering judgment. Some tasks are so complicated that each step in the SOP is abbreviated to reduce verbiage and entered in the checklist as a step. Other tasks may be routine enough that many SOP steps are omitted from the checklist. A checklist may be used to document system parameters required by research or may be used as a tool that requires the operator to ensure that a level of operations is complete and the system is ready to continue to the next level of operations.

An example of a complicated task would be the preheat of the 20" SWT. In this task, the preheat pressure is close to the pressure that will lift relief devices. If the SOP's 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 include most of the steps from the SOP.

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 form 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.

The following list further establishes instructions for generation of checklists:

(1) A checklist is a CCD document and requires generation of a CNS for modification.

(2) Checklist Format

(a) 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 push button and verify that the OFF half is

EXTINGUISHED and the ON half becomes ILLUMINATED." The step could be abbreviated in the checklist to "Start rotovalve hydraulic pump and verify ON light becomes ILLUMINTATED." in the checklist.

(b) WARNINGS that are in the SOP shall be in the checklist and may be abbreviated to reduce the verbiage as long as the meaning remains clear.

(c) CAUTIONS that are in the SOP shall be in the checklist and may be abbreviated to reduce the verbiage as long as the meaning remains clear.

(d) 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 the verbiage as long as the meaning remains clear.

(e) When used, sign off spaces shall be located on the checklist at a location agreed to by the FSH, FC, Operators, and the Safety Office. The preferred location is to the left of the step number.

(e) Mature systems may have "placard" type checklists that are conveniently posted at equipment to be operated.

(3) 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 cognizant research personnel. The Safety Office does not retain completed checklists.