U.S. Department of Energy
Office of River Protection
Mr. Michael K. Barrett
Contracting Officer
P.O. Box 450, MSIN H6-60
Richland, Washington 99352

CCN: 027636

Dear Mr. Barrett:

CONTRACT NO. DE-AC27-01RV14136 – FOR INFORMATION, INCORPORATION OF SAFETY REQUIREMENTS DOCUMENT AND INTEGRATED SAFETY MANAGEMENT PLAN PAGE CHANGES PER U.S. DEPARTMENT OF ENERGY APPROVAL OF AUTHORIZATION BASIS CHANGE NOTICES ABCN-24590-01-00004, REVISION 2, AND 24590-WTP-ABCN-ESH-01-013, REVISION 1

References: 1) CCN 028213, Letter, R. C. Barr, OSR, to R. F. Naventi, BNI, "Office of Safety Regulation (OSR) Approval of Bechtel National, Inc (BNI) Authorization Basis Change Notice, 24590-WTP-ABCN-ESH-01-013, Revision 1, Codes and Standards Update/NPH Design Requirements," 02-OSR-0019, dated January 30, 2002

2) CCN 028170, Letter, R. C. Barr, OSR, to R. F. Naventi, BNI, "Approval of Bechtel National, Inc. (BNI) Authorization Basis Change Notice, ABCN-24590-01-00004, Rev. 2., "Identification of Safety Analysis Report (SAR) Format and Content," 02-OSR-0034, dated January 29, 2002

Attached for your information are page changes for the Hanford Tank Waste Treatment and Immobilization Plant Safety Requirements Document (SRD), Revisions 0b and 0c, and the Integrated Safety Management Plan (ISMP), Revision 0e. These page changes were approved by the U.S. Department of Energy, Office of Safety Regulation (OSR) as noted in the above reference letters.

The page changes were a result of OSR approval of the Authorization Basis Change Notices (ABCN) listed below:

- ABCN-24590-01-00004, Rev. 2, *Identification of Safety Analysis Report (SAR) Format and Content* (SRD Volume II, Revision 0b, and ISMP, Revision 0e)

- 24590-WTP-ABCN-ESH-01-013, Rev. 1, *Codes & Standards Update / NPH Design Requirements* (SRD Volume II, Revision 0c)

An electronic copy of page changes for the SRD and ISMP revisions is also provided for DOE OSR's information and use.

Please contact Mr. Bill Spezialetti at (509) 371-4654 for any questions or comments on this transmittal.

Very truly yours,

A. R. Veirup
Prime Contract Manager

TBR/slr

Attachments:
1) *Safety Requirements Document*, 24590-WTP-SRD-ESH-01-001-02, Revision 0b
2) *Integrated Safety Management Plan*, 24590-WTP-ISMP-ESH-01-001, Revision 0e
3) *Safety Requirements Document*, 24590-WTP-SRD-ESH-01-001-02, Revision 0c

Document title:	**Safety Requirements Document Volume II**
Contract number:	DE-AC27-01RV14136
Department:	Environmental, Safety, and Health
Document number:	24590-WTP-SRD-ESH-01-001-02, Rev 0b
Date of issue:	19 February 2002
Issue status:	Approved

History Sheet

Rev	Date	Reason for revision	Revised by
0	21 Sep 2001	Supersedes BNFL-5193-SRD-01-02 Rev 5. Incorporates 24590-WTP-ABCN-ESH-01-017 Rev 0 changes (contractor-approved ABCN).	K Gibson
0a	4 Oct 2001	Incorporates ABCN-24590-01-00006 Rev 0 changes as partially approved by DOE Letter 01-OSR-0311 (CCN 023253) and contractor approved as revised ABCN-24590-01-00006, Rev 1.	K Gibson
0b	19 Feb 2002	Incorporates ABCN-24590-01-00004 Rev 2 changes as approved (with editorial changes specified) by DOE Letter 02-OSR-0034 (CCN 028170).	K Gibson

Revision Status

Page No.	Rev.	Page No.	Rev.	Page No.	Rev.	Page No.	Rev.
i	0b	4-15	0	7-4	0	9-11	0a
ii	0b	4-16	0a	7-5	0	9-12	0a
iii	0b	4-17	0	7-6	0a	9-13	0a
iv	0b	4-18	0	7-7	0a	9-14	0a
v	0a	4-19	0	7-8	0a	A-i	0
vi	0b	4-20	0	7-9	0	A-ii	0
1-1	0a	4-21	0	7-10	0	A-1	0
1-2	0	4-22	0	7-11	0a	A-2	0
1-3	0a	4-23	0	7-12	0a	A-3	0
1-4	0	4-24	0	7-13	0	A-4	0
2-1	0	4-25	0	7-14	0a	A-5	0a
2-2	0	4-26	0	7-15	0	A-6	0
2-3	0a	4-27	0	7-16	0	A-7	0
3-1	0a	4-28	0	7-17	0a	A-8	0
3-2	0a	4-29	0	7-18	0	A-9	0
3-3	0a	4-30	0	7-19	0a	A-10	0
3-4	0a	4-31	0	7-20	0a	A-11	0a
3-5	0a	4-32	0a	7-21	0a	A-12	0
3-6	0	5-1	0	7-22	0	A-13	0
3-7	0	5-2	0	7-23	0	A-14	0
3-8	0	5-3	0	7-24	0	A-15	0
3-9	0	5-4	0	7-25	0a	A-16	0
4-1	0a	5-5	0	7-26	0a	A-17	0
4-2	0	5-6	0	7-27	0a	A-18	0
4-3	0	5-7	0	8-1	0	A-19	0
4-4	0	5-8	0	9-1	0	A-20	0
4-5	0a	5-9	0	9-2	0	B-i	0
4-6	0	5-10	0	9-3A	0b	B-ii	0
4-7	0	5-11	0	9-3B	0b	B-1	0
4-8	0a	5-12	0	9-4	0b	B-2	0
4-9	0	5-13	0	9-5	0a	B-3	0
4-10	0	6-1	0a	9-6	0	B-4	0
4-11	0	6-2	0a	9-7	0	B-5	0
4-12	0	7-1	0	9-8	0	B-6	0
4-13	0	7-2	0	9-9	0	B-7	0
4-14	0	7-3	0a	9-10	0a	B-8	0

Page No.	Rev.	Page No.	Rev.	Page No.	Rev.	Page No.	Rev.
B-9	0	C-3	0	D-6	0	G-6*	0b
B-10	0	C-4	0	D-7	0	G-7*	0b
B-11	0	C-5	0	D-8	0	G-8*	0b
B-12	0	C-6	0	D-9	0	G-9*	0b
B-13	0	C-7	0	D-10	0	G-10*	0b
B-14	0	C-8	0	D-11	0	G-11*	0b
B-15	0	C-9	0	D-12	0	G-12*	0b
B-16	0	C-10	0	E-i	0	G-13*	0b
B-17	0	C-11	0	E-1	0	G-14*	0b
B-18	0	C-12	0	E-2	0	G-15*	0b
B-19	0	C-13	0	F-i	0	G-16*	0b
B-20	0	C-14	0	F-ii	0	G-17*	0b
B-21	0	C-15	0	F-1	0	G-18*	0b
B-22	0	C-16	0	F-2	0	G-19*	0b
B-23	0	D-i	0	G-i*	0b	G-20*	0b
B-24	0	D-ii	0	G-ii*	0b	G-21*	0b
B-25	0	D-1	0	G-1*	0b	G-22*	0b
C-i	0	D-2	0	G-2*	0b	G-23*	0b
C-ii	0	D-3	0	G-3*	0b	G-24*	0b
C-1	0	D-4	0	G-4*	0b	G-25*	0b
C-2	0	D-5	0	G-5*	0b		

* These pages added at this revision; therefore, no revision bars are used to indicate changes.

Approved by: _____ _____ Date: _____
(Print name) (Sign)

CONTENTS

1.0 Radiological, Nuclear and Process Safety Objectives....1-1
2.0 Radiological and Process Standards....2-1
3.0 Nuclear and Process Safety....3-1
3.1 Hazards Analysis....3-1
3.2 Accident Analysis....3-6
3.3 Criticality....3-7
4.0 Engineering and Design....4-1
4.1 General Design....4-3
4.2 Confinement Design....4-11
4.3 Engineered Safety Systems....4-13
4.4 Electrical and Mechanical Systems....4-17
4.5 Fire Protection....4-26
5.0 Radiation Protection....5-1
5.1 Occupational Radiation Protection....5-1
5.2 Occupational Radiation Protection Design....5-6
5.3 Environmental Radiation Protection....5-7
5.4 Environmental Radiological Monitoring....5-12
6.0 Startup....6-1
7.0 Management and Operations....7-1
7.1 Management and Organization/Staffing....7-3
7.2 Training and Procedures....7-5
7.3 Quality Assurance Program....7-9
7.4 Unreviewed Safety Questions....7-14
7.5 Conduct of Operations....7-16
7.6 Maintenance....7-17
7.7 Reporting and Incident Investigation....7-20
7.8 Emergency Preparedness....7-25
8.0 Deactivation and Decommissioning....8-1
9.0 Documentation and Submittals....9-1
9.1 Safety Analysis Reports....9-3
9.2 Technical Safety Requirements....9-6
9.3 Risk Management Plan (this section has been deleted)....9-10

APPENDICES

Appendix A Implementing Standard for Safety Standards and Requirements Identification.....A-i
Appendix B Implementing Standard for Defense in Depth .....B-i
Appendix C Implementing Standards .....C-i
Appendix D Radiological Exposure Standards for the RPP-WTP Project .....D-i
Appendix E Reliability, Availability, Maintainability, and Inspectability (RAMI).....E-i
Appendix F Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning..... F-i
Appendix G Ad Hoc Implementing Standard for Safety Analysis Reports.....G-i

1.0 Radiological, Nuclear and Process Safety Objectives

Safety Criterion: 1.0 - 1

A comprehensive radiological and process safety management program shall be used to eliminate or reduce the incidence, or mitigate the consequences of, accidental radioactive or chemical releases, process fires, and process explosions. This program shall address management practices, technologies, and procedures. Radiological and process safety management shall confirm that the facility is properly designed, the integrity of the design is maintained, and the facility is operated according to the safe manner intended.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 4.1 Safety Management Processes
Chapter: 5.0 Process Safety Management

Regulatory Basis

DOE/RL-96-0006 5.1.1 Process Safety Management
DOE/RL-96-0006 5.1.2 Process Safety Objective

Safety Criterion: 1.0 - 2

Principal emphasis shall be placed on the prevention of accidents, particularly any that could cause an unacceptable release, as the primary means of achieving safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2

Regulatory Basis

DOE/RL-96-0006 4.1.1.2 Defense in Depth-Prevention

Safety Criterion: 1.0 - 3

The risk, to an average individual within 1 mile of the RPP-WTP Controlled Area Boundary, of prompt fatalities that might result from an accident shall not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents which members of the U.S. population generally are exposed.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 3.1.2 Accident Risk Goal

Safety Criterion: 1.0 - 4

The risk, to the public and workers within 16 km (10 miles) of the RPP-WTP, of cancer fatalities that might result from RPP-WTP operations shall not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks to which members of the U.S. population generally are exposed.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

test change

Regulatory Basis

DOE/RL-96-0006 3.1.1 Operations Risk Goal

Safety Criterion: 1.0 - 5

The risk to workers within the RPP-WTP Controlled Area Boundary, of fatality from radiological exposure that might result from an accident, shall not be a significant contributor to the overall occupational risk of fatality to workers.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 3.1.3 Worker Accident Risk Goal

Safety Criterion: 1.0 - 6

Measures in the design and operation of the facility to protect the public, workers, and environment against accident conditions shall be evaluated using an acceptable approach to demonstrate that they perform their intended purpose with high confidence.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 3.3.1 Public Protection

DOE/RL-96-0006 3.3.2 Worker Protection

Safety Criterion: 1.0 - 7

To compensate for potential human and equipment failures, a defense-in-depth strategy shall be applied to the facility commensurate with the hazards; such that, as appropriate to control the risk, safety is vested in multiple, independent safety provisions, no one of which is to be relied upon excessively to protect the public, the workers, or the environment. This strategy shall be applied to the design and operation of the facility.

Implementing Codes and Standards

ANSI/ANS 58.9-1981 Single Failure Criteria for Light Waster Reactor Safety-Related Fluid Systems
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety 4.1.1.2
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006 *4.1.1.1 Defense in Depth-Defense in Depth*

Safety Criterion: 1.0 - 8

Structures, systems, and components (SSCs) that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public are classified as Important to Safety. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation). This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of Important to Safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Important to Safety includes SSCs designated as Safety Design Class and Safety Design Significant.

Safety Design Class SSCs includes those that, by performing their specified safety function, prevent workers or the maximally exposed member of the public from receiving a radiological or chemical exposure that exceeds the exposure standards defined in the SRD. Those features credited for the prevention of a criticality event are also designated as Safety Design Class.

Safety Design Significant SSCs are those needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that can, if they fail or malfunction, place frequent demands on, or adversely affect the function of, Safety Design Class SSCs.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006	*3.3.1*	*Public Protection*
DOE/RL-96-0006	*3.3.2*	*Worker Protection*

Safety Criterion: 1.0 - 9

The RPP-WTP Contractor shall accept responsibility for the safety of the RPP-WTP.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 1.0 Project Safety Approach
Section: 11.1 Design and Construction Phase
Section: 11.2 Operations Phase

Regulatory Basis

DOE/RL-96-0006	*4.1.2.1*	*Safety Responsibility-Safety Responsibility*
DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*
DOE/RL-96-0006	*5.1.3*	*Process Safety Responsibility*

Safety Criterion: 1.0 - 10

In addition to the Safety Criteria contained herein, compliance with all requirements of 10 CFR 830.120 and 10 CFR 835 shall be achieved absent the granting of an exemption request to any specific requirement therein.

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location*
10 CFR 835	*Occupational Radiation Protection*	*Location: 1*
DE-AC06-96RL13308	*Part I Section C.5 Table S4-1*	

2.0 Radiological and Process Standards

Safety Criterion: 2.0 - 1

The following Radiological Dose Standards shall be applied to protect the public and workers from RPP-WTP radiological hazards.

Table 2-1. Radiological Exposure Standards Above Normal Background (Sheet 1)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Normal Events Events that occur regularly in the course of facility operation (e.g., normal facility operations); including routine and preventive maintenance activities.	>0.1	Normal modes of operating facility systems should provide adequate protection of health and safety.	≤5 rem/yr ≤50 rem/yr any organ, skin, or extremity ≤15 rem/yr lens of eye ≤1.0 rem/yr ALARA design objective per 10CFR835.1002(b)(1)	≤5 rem/yr ≤1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b)(1)	≤10 mrem/yr (airborne pathway) ≤100 mrem/yr (all sources) ≤100 mrem/yr (public in the controlled area) ≤25 mrem/yr (radioactive waste)
Anticipated Events Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	$10^{-2}<f\leq10^{-1}$	The facility should be capable of returning to operation without extensive corrective action or repair.	≤5 rem/event (2,3) 1.0 rem/event design action threshold (4)	≤5 rem/event (2, 3) 1.0 rem/event design action threshold(4)	≤100 mrem/event(3)
Unlikely Events Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	$10^{-4}<f\leq10^{-2}$	The facility should be capable of returning to operation following potentially extensive corrective action or repair, as necessary.	≤25 rem/event(2,3)	≤25 rem/event(2, 3)	≤5 rem/event(3)

Table 2-1. Radiological Exposure Standards Above Normal Background (Sheet 2)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Extremely Unlikely Events Events that are not expected to occur during the life of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.	$10^{-6}<f\leq10^{-4}$	Facility damage may preclude returning to operation.	≤25 rem/event(2,3)	≤25 rem/event(2,3)	≤25 rem/event ≤5 rem/event target(3) ≤300 rem/event to thyroid
Location of Receptor			Within the RPP-WTP Controlled Area Boundary	The most limiting location at or beyond the RPP-WTP Controlled Area Boundary	The most limiting location along the near river bank/ Hwy240/ southern boundary

Notes
(1) In addition to meeting the listed design objective of 10 CFR 835.1002(b), the inhalation of radioactive material by workers and collocated workers under normal conditions is kept ALARA through the control of airborne radioactivity as described in 10 CFR 835.1002(c).

(2) In addition to meeting the listed worker and collocated worker exposure standards for accidents, the Worker Accident Risk Goal is satisfied through the calculation of the risk from accidents with accident prevention and mitigation features added as necessary to meet the Goal.

(3) In addition to meeting the listed exposure standards for accidents, the approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below standards to account for uncertainties in the analysis, and to provide for sufficient design margin and operational flexibility.

(4) When a calculated accident exposure exceeds this threshold, then appropriate actions are taken. These include carrying out a less bounding (i.e., more realistic) evaluation to show that the accident consequences will be below the threshold or evaluating additional safeguards for cost-effectiveness and/or feasibility. This threshold is not a limit; it does not require the implementation of additional preventative or mitigative features if they are not both cost-effective and feasible.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 2.1 Individual (Dose Standards Above Normal Background)

Safety Criterion: 2.0 - 2

The following dose standards shall be applied to protect the public and workers from RPP-WTP chemical hazards.

Releases exposing the offsite public to ERPG-2 concentrations (AIHA 1999)

Releases exposing the co-located worker to ERPG-3 concentrations (AIHA 1999)

Accidents affecting the facility worker that could cause in-patient hospitalization of at least 3 facility workers, or at least a single fatality.

Where ERPG values have not been published, the DOE Temporary Emergency Exposure Limits (TEELs) may be used as substitute ERPGs.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 2.0 - 3

In addition to the dose limits specified for the public in Safety Criterion 2.0-1 Table 2-1, the dose in any unrestricted area from external sources shall not exceed 0.002 rem in any one hour.

Implementing Codes and Standards

DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

WAC 246-221 Radiation Protection Standards Location: 060 (1)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 040 (2)

3.0 Nuclear and Process Safety

3.1 Hazards Analysis

Safety Criterion: 3.1 - 1

An initial process hazard analysis (hazard evaluation) shall be performed using acceptable industry practices. The analysis shall include consideration of both chemical and radiological hazards. The process hazard analysis shall be appropriate to the complexity of the process and shall identify, evaluate, and document the design features which control the hazards involved in the process.

The process hazard analysis shall be performed by a team with expertise in engineering and process operations, and the team shall include at least one member who has experience and knowledge specific to the process being evaluated. Also, one member of the team must be knowledgeable in the specific process hazard analysis methodology being used.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 2

A compilation of written process safety information appropriate to the stage of design being considered shall be completed to support the process hazard analysis. The compilation of written process safety information enables the employer and the employees involved in operating the process to identify and understand the hazards posed by those processes involving radioactive materials and process chemicals considered to pose a hazard. This process safety information shall include information pertaining to the hazards of the materials used or produced by the process, information pertaining to the technology of the process, and information pertaining to the equipment in the process.

(1) Information pertaining to the hazards of the materials in the process including:
   - (a) Toxicity information
   - (b) Permissible exposure limits
   - (c) Physical data
   - (d) Reactivity data
   - (e) Corrosivity data
   - (f) Thermal and chemical stability data
   - (g) Hazardous effects of inadvertent mixing of different materials that could foreseeably occur

(2) Information pertaining to the technology of the process including at least the following:
   (a) A block flow diagram or simplified process flow diagram
   (b) Process chemistry
   (c) Maximum intended inventory
   (d) Safe upper and lower limits for such items as temperatures, pressures, flows or compositions
   (e) An evaluation of the consequences of deviations, including those affecting the safety and health of employees

(3) Information pertaining to the equipment in the process including:
   (a) Materials of construction
   (b) Process drawings or piping and instrument diagrams (P&IDs)
   (c) Electrical classification
   (d) Relief system design and design basis
   (e) Ventilation system design
   (f) Design codes and standards employed
   (g) Material and energy balances
   (h) Safety systems (e.g. interlocks, detection or suppression systems)

The records shall be maintained documenting that equipment complies with recognized and generally accepted good engineering practices. The safety information shall be kept up-to-date.

Implementing Codes and Standards

Regulatory Basis

DOE/RL-96-0006	*5.2.1*	*Process Safety Information*
DOE/RL-96-0006	*5.2.2*	*Process Hazard Analysis*

Safety Criterion: 3.1 - 3

The process hazard analysis shall address:

(1) The hazards of the process

(2) Engineering and administrative controls applicable to the hazards and their interrelationships such as appropriate application of detection methodologies to provide early warning of releases. (Acceptable detection methods might include process monitoring and control instrumentation with alarms, and detection hardware.)

(3) Consequences of failure of engineering and administrative controls

(4) Facility siting

(5) Human factors

(6) A qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace

(7) Common-mode and common-cause failure events

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 4

The hazard analysis shall be performed in accordance with the following requirements:

(1) The consequences of unmitigated releases of radioactive material and process chemicals considered to pose a hazard shall be evaluated.

(2) The hazard analysis shall be based on an inventory of all radioactive and hazardous nonradioactive materials that are stored, utilized, or may be formed within the facility.

(3) The hazard analysis shall identify energy sources or processes that might contribute to the generation or uncontrolled release of radioactive or process chemicals considered to pose a hazard. The hazard analysis shall estimate the consequences of accidents in which the facility or process and/or materials in the inventory are assumed to interact, react, or be released in a manner to produce a threat or challenge to the health and safety of individuals on-site and off site.

(4) The risks that hazardous inventories and energy sources present shall be evaluated by consideration of normal operation (including startup, testing, and maintenance), anticipated operational occurrences, and accident conditions. The identification of anticipated operational occurrences and accident conditions shall consider internal events (i.e., equipment failure and human error), external events (e.g., nearby facilities and transportation), and natural phenomena.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006	*3.3.3*	*Accident Vulnerability Mitigation*
DOE/RL-96-0006	*5.2.2*	*Process Hazard Analysis*

Safety Criterion: 3.1 - 5

A written plan of action shall be developed regarding employee participation in the conduct and development of process hazards analyses and on the development of process safety management. Employees and their representatives shall be consulted on the conduct and development of process hazards analyses and on the development of the other elements of process safety management. Employees and their representatives shall be provided access to process hazard analyses and other information developed related to process safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

Safety Criterion: 3.1 - 6

A system shall be established to promptly address the hazard analysis team's findings and recommendations; assure that the recommendations are resolved in a timely manner; and that the resolution is documented. The contractor shall document what actions are to be taken; complete actions; develop a written schedule of when these actions are to be completed; communicate the actions to operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 7

The process hazard analysis shall be updated to reflect changes concurrently with the annual update of the FSAR by a qualified team, to assure that the process hazard analysis is consistent with the current process.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation
Section: 5.6.2 Updating of the Hazard Analysis Report

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 8

Employers shall retain process hazards analyses and updates or revalidations as well as the documented resolution of any recommendations for the life of the process.

Implementing Codes and Standards

Regulatory Basis

3.2 Accident Analysis

Safety Criterion: 3.2 - 1

Acceptable risk analyses shall be applied during the design to delineate provisions for the prevention and mitigation, including emergency preparedness and response, of otherwise risk-dominant events.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3 Description of the Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 4.2.1.2 Design-Risk Assessment

3.3 Criticality

Safety Criterion: 3.3 - 1

The facility shall be designed and operated in a manner that prevents nuclear criticality.

Implementing Codes and Standards

ANSI/ANS 8.1-1983 (R 1988) Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors

ANSI/ANS 8.19-1996 Administrative Practices for Nuclear Criticality Safety

Regulatory Basis

DOE/RL-96-0006 4.2.2.5 Proven Engineering Practices/Margins-Criticality

Safety Criterion: 3.3 - 2

The design of handling, packaging, transfer, and storage systems must include margins of safety for the nuclear criticality parameters that are commensurate with the uncertainties in the data and methods used in calculations and in the nature of the immediate environment under accident conditions.

The multiplication factor (k<eff>), including all biases and uncertainties at a 95% confidence level, shall be shown to not exceed 0.95 under all credible normal, off-normal, and accident conditions.

Safety Criterion: 3.3 - 3

Process designs shall incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible. Protection shall be provided by either:

(1) the control of two independent process parameters (which is the preferred approach, when practical, to prevent common-mode failure), or

(2) a system of multiple controls on a single process parameter.

The number of controls required for a single controlled process parameter shall be based upon control reliability and any features that mitigate the consequences of control failure. In all cases, no single credible event or failure shall result in the potential for a criticality accident.

An exception to the application of double contingency, where single contingency operations are permissible, is presented in paragraph 5.1 of ANSI/ANS-8.10-1983, R88. This exception applies to operations with shielding and confinement (e.g., hot cells or other shielded facilities).

Double contingency shall be demonstrated by documented evaluations.

Safety Criterion: 3.3 - 4

Where a sufficient quantity of fissionable material is being processed such that criticality safety is a concern, passive engineered controls, such as geometry control, shall be considered as the preferred control method. Where passive engineered control is not feasible, the preferred order of controls is active engineered controls followed by administrative controls. The double contingency analysis shall justify the chosen controls. Full advantage may be taken of any nuclear characteristics of the process materials and equipment. The geometry must be considered as water moderated and reflected unless it can be shown the presence of water is not credible. All dimensions, nuclear properties, and other features upon which reliance is placed shall be documented and verified prior to beginning operations, and control shall be exercised to maintain them.

Safety Criterion: 3.3 - 5

To protect against an uncontrolled nuclear criticality incident, nuclear criticality safety considerations and controls shall be evaluated for accidents, normal operations, and before any significant operational changes are made.

Safety Criterion: 3.3 - 6

Criticality Accident Alarm Systems (CAS) and Criticality Detection Systems (CDS) shall be required as follows:

(1) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material and the probability of a criticality accident is greater than 1E-06 per year, a CAS conforming to ANSI/ANS-8.3-1986 shall be provided to cover occupied areas in which the expected dose exceeds 12 rads (0.12 greys) in free air, where a CAS is defined to include a criticality accident detection device and a personnel evacuation alarm.

(2) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material and the probability of a criticality accident is greater than 1E-06 per year, but there are no occupied areas in which the expected dose exceeds 12 rads (0.12 greys) in free air, a CDS shall be provided, where a CDS is defined to be an appropriate criticality accident detection device but without an immediate evacuation alarm. The CDS response time should be sufficient to allow for appropriate process-related mitigation and recovery actions. Appropriate response guidance to minimize personnel exposure shall be provided.

(3) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material, but a criticality accident is determined to be impossible due to the physical form of the fissionable material, or the probability of occurrence is determined to be less than 1E-06 per year, neither a CAS nor a CDS is required. Neither a CAS nor a CDS is required for fissionable material during shipment when packaged in approved shipping containers, or when packaged in approved shipping containers awaiting transport provided that no other operation involving fissionable material not so packaged is permitted on the shipping dock or in the shipment area.

(4) If a criticality accident is possible wherein a slow (i.e., quasistatic) increase in reactivity could occur leading from subcriticality to criticality to self-shutdown without initiating emplaced criticality alarms, CASs should be supplemented by warning devices such as audible personnel dosimeters (e.g., pocket chirpers/flashers, or their equivalents), area radiation monitors, area dosimeters, or integrating CASs to aid in protecting workers against the consequences of slow criticality accidents.

(5) Neither a CAS nor a CDS is required to be installed for handling or storage of fissionable material when sufficient shielding exists that is adequate to protect personnel (e.g., hot cells); however, a means to detect fission product gases or other volatile fission products shall be provided in occupied areas immediately adjacent to such shielded areas, except for systems where no fission products are likely to be released.

Note: The frequency of 1E-06 per year is used as a measure of credibility and does not require a probabilistic risk assessment be performed. Reasonable grounds for incredibility may be presented on the basis of commonly accepted engineering judgement.

Table 3-1. Inventory of Fissionable Material[1]

Isotope	Inventory in Individual Unrelated Area
U-235	700g
U-233	520g
Pu-239	450g
Any Combination of above Isotopes	450g

[1] Per ANSI/ANS-8.3-1986 paragraph 4.2.1

Safety Criterion: 3.3 - 7

The monitoring system shall be capable of detecting a criticality that produces an absorbed dose in soft tissue of 20 rads (0.20 greys) of combined neutron and gamma radiation at an unshielded distance of 2 meters from the reacting material within one minute.

Safety Criterion: 3.3 - 8

Coverage of all areas requiring detection may be provided by a single detector.

4.0 Engineering and Design

Safety Criterion: 4.0 - 1

Formal configuration management shall be applied to all facility activities through deactivation of the RPP-WTP to ensure that programmatic objectives, including safety, are fully achieved. Work shall be performed and controlled according to pre-approved plans and procedures that clearly delineate responsibility. Documented records shall be retained.

Implementing Codes and Standards
ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis
DOE/RL-96-0006 4.1.5.1 Configuration Management-Formal Configuration Management

Safety Criterion: 4.0 - 2

Written procedures shall be established and implemented to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures; and, changes to facilities that affect a covered process. The procedures shall assure that the following considerations are addressed prior to any change:

(1) The technical basis for the proposed change

(2) Impact of change on safety and health

(3) Modifications to operating procedures

(4) Necessary time period for the change

(5) Authorization requirements for the proposed change

Employees involved in operating a process and maintenance and subcontract employees whose job tasks will be affected by a change in the process shall be informed of, and trained in, the change prior to start-up of the process or affected part of the process. If a change covered by this paragraph results in a change in the process safety information, such information shall be updated accordingly. If a change covered by this paragraph results in a change in operating procedures or practices, such procedures or practices shall be updated accordingly.

Implementing Codes and Standards
ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis
DOE/RL-96-0006 5.2.9 Management of Change

Safety Criterion: 4.0 - 3

A system shall be used to control and maintain accurate as-built records for Important to Safety SSCs through deactivation of the facility.

Implementing Codes and Standards

ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis

DOE/RL-96-0006 *4.1.5.3 Configuration Management-Design Documentation*

4.1 General Design

Safety Criterion: 4.1 - 1

The facility design shall provide for the prevention and mitigation of the risks associated with radiological and chemical material inventories and energy sources. The facility design shall include consideration of normal operation (including startup, testing and maintenance), anticipated operational occurrences, external events, and accident conditions.

Prevention shall be the preferred means of achieving safety.

Defense-in-depth shall be applied commensurate with the hazard to provide multiple physical and administrative barriers against undue radiation and chemical exposure to the public and workers.

Implementing Codes and Standards

ANSI/ANS 58.9-1981 Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety 4.1.1.2
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006	*4.1.1.1*	*Defense in Depth-Defense in Depth*
DOE/RL-96-0006	*4.1.1.2*	*Defense in Depth-Prevention*
DOE/RL-96-0006	*4.2.1.1*	*Design-Safety Design*

Safety Criterion: 4.1 - 2

Structures, systems, and components designated as Important to Safety shall be designed, fabricated, erected, constructed, tested, inspected, and maintained to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components designated as Important to Safety shall be maintained through deactivation of the facility.

Items and processes shall be designed using sound engineering/scientific principles and appropriate standards.

Design features that enhance the margin of safety through simplified, inherently safe, passive, or other highly reliable means to accomplish the specified safety function should be employed to the maximum extent practical.

Design work, including changes, shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled. The adequacy of design products shall be verified or validated by individuals or groups other than those who performed the work. Verification and validation work shall be completed before approval and implementation of the design.

Safety technologies incorporated into the facility design should have been proven by experience or testing and should be reflected in approved codes and standards. Significant new design features should be introduced only after thorough research and model or prototype testing at the component, system, or facility level, as appropriate, to achieve the necessary level of confidence that the design feature will perform as expected.

Implementing Codes and Standards

ACI 318-99 Building Code Requirements for Structural Concrete
ACI 318R-99 Commentary on Building Code Requirements for Structural Concrete
ACI 349-97 Code Requirements for Nuclear Safety-Related Concrete Structures
ACI 349R-97 Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures
AISC MO16-89 Manual for Steel Construction - Allowable Stress Design, Ninth Edition
ANSI/AISC N690-94 Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities
ASCE 4-98 (Draft) Seismic Analysis of Safety-Related Nuclear Structures and Commentary
ASCE 7-95 Minimum Design Loads for Buildings and Other Structures
DOE-STD 1020-94 (Change 1, 1996) Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities
1997 UBC Uniform Building Code
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
ACI 530-95, Building Code Requirements for Masonry Structures and Commentary
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
ISO 10007 Quality Management - Guidelines for Configuration Management
ASTM D3740, Standard Practice for Minimum Requirements for Agencies Engaged in the Testing and/or Inspection of Soil and Rock as Used in Engineering Design and Construction
ASTM D2922, Standard Test Method for Laboratory Determination of Moisture Content of Soil
ASTM D3017, Standard Test Method for Water Content of Soil and Rock in Place by Nuclear Methods

Regulatory Basis

DOE/RL-96-0006	*4.1.2.4*	*Safety Responsibility-Operating Experience and Safety Research*
DOE/RL-96-0006	*4.1.5.1*	*Configuration Management-Formal Configuration Management*
DOE/RL-96-0006	*4.1.6.2*	*Quality Assurance-Established Techniques and Procedures*
DOE/RL-96-0006	*4.2.2.1*	*Proven Engineering Practices/Margins-Proven Engineering Practices*
DOE/RL-96-0006	*4.2.2.3*	*Proven Engineering Practices/Margins-Safety System Design and Qualification*
DOE/RL-96-0006	*4.2.5.1*	*Inherent/Passive Safety Characteristics-Safety Margin Enhancement*

Safety Criterion: 4.1 - 3

This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) that are Important to Safety and have NPH safety functions.

SSCs designated as Important to Safety (i.e., Safety Design Class and Safety Design Significant) shall be designed to withstand the effects of NPH events such as earthquakes, wind, and floods without loss of capability to perform specified safety functions required as the result of the NPH events. This includes both the front line and support systems that must function for a NPH event such that the public, collocated worker, or facility worker exposure standards of Safety Criterion 2.0-1 or 2.0-2 are not exceeded.

SSCs that are designated Safety Design Class (excepting those so designated based solely on chemical hazards) and that are required to perform a safety function as a result of a given NPH shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. These SSCs are designated Seismic Category I (SC-I) for earthquakes and Performance Category 3 (PC-3) for other NPH. SSCs designated as Safety Design Class based solely on a safety function relative to chemical hazards shall be designated as SC-III for earthquakes, and shall be designed to meet PC-3 requirements for other NPH events.

SSCs that are designated Safety Design Significant whose continued function is not required for an NPH event, but whose failure as a result of an NPH event could reduce the functioning of a Safety Design Class SSC such that exposure standards might be exceeded, shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. For these SSCs, however, for seismic response only, credit may be taken for inelastic energy absorption per Table 2-4 of DOE-STD-1020-94. These SSCs are designated SC-II for earthquakes and PC-3 for other NPH. SSCs designated as Safety Design Significant based solely on a safety function relative to chemical hazards shall be designated as SC-III for earthquakes, and shall be designed to meet PC-3 requirements for other NPH events.

For any SSC included under this criterion, other NPH loads (for which the SSC has no safety function) may be taken from Safety Criterion 4.1-4 and Table 4-2 in lieu of Safety Criterion 4.1-3 and Table 4-1. SSCs designated as Safety Design Significant based solely on safeguarding a safety function relative to chemical hazards shall be designated SC-III for earthquakes, and shall be deisgned to meet PC-2 requirements for other NPH events.

Table 4-1. Natural Phenomena Design Loads for Important to Safety SSCs with NPH Safety Functions

Hazard	Load	Source Document for Load
Seismic	DBE with 0.26 *g* horizontal PGA and 0.18 *g* vertical PGA See Figures 4-1 and 4-2	WHC-SD-W236A-TI-002 [a] DOE-STD-1020-94[b]
Straight wind	111 mi/hr , 3-second gust, at 33 ft above ground, Importance factor, I=1.0	DOE Newsletter [c]
Wind Missile	2x4 timber plank, 15 lb at 50 mi/hr (horiz), Max height 30 ft	DOE-STD-1020-94 [b]
Tornado and Tornado Missiles	Not Applicable	DOE-STD-1020-94 [b]
Volcanic ash	12.5 lb/ft^2	HNF-SD-GN-ER-501 [d]
Flooding	Dry site for river flooding Local precipitation: 4 in. for 6 hours	HNF-SD-GN-ER-501 [d]
Snow	15.0 lb/ft^2 snow load	HNF-SD-GN-ER-501 [d]

[a] Geomatrix, 1996, *Probabilistic Seismic Hazard Analysis DOE Hanford Site, Washington,* WHC-SD-W236A-TI-002, Rev.1A, prepared for Westinghouse Hanford Company, Richland, Washington.

[b] DOE STD-1020-94, (1996, Change 1) *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, U.S. Department of Energy, Washington, D.C., 1996.

[c] DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98.

[d] HNF-SD-GN-ER-501, Rev. 1, "Natural Phenomena Hazards, Hanford Site, South-Central Washington", Westinghouse Hanford Company.

Figure 4-1

RPP-WTP DBE Horizontal Response Spectra
(0.50%, 2%, 3%, 4%, 5%, 7%, 10%, 12% Damping)

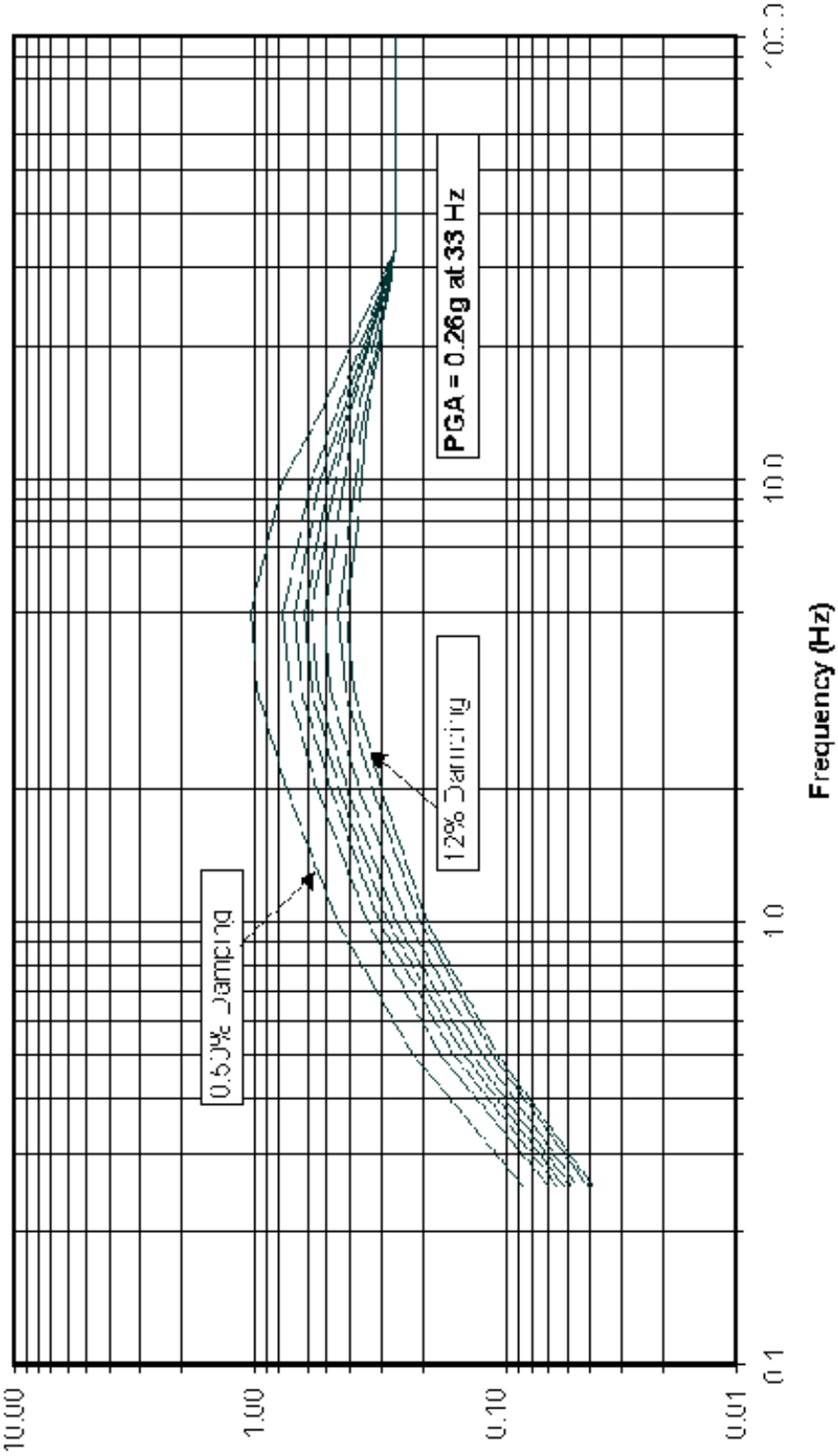
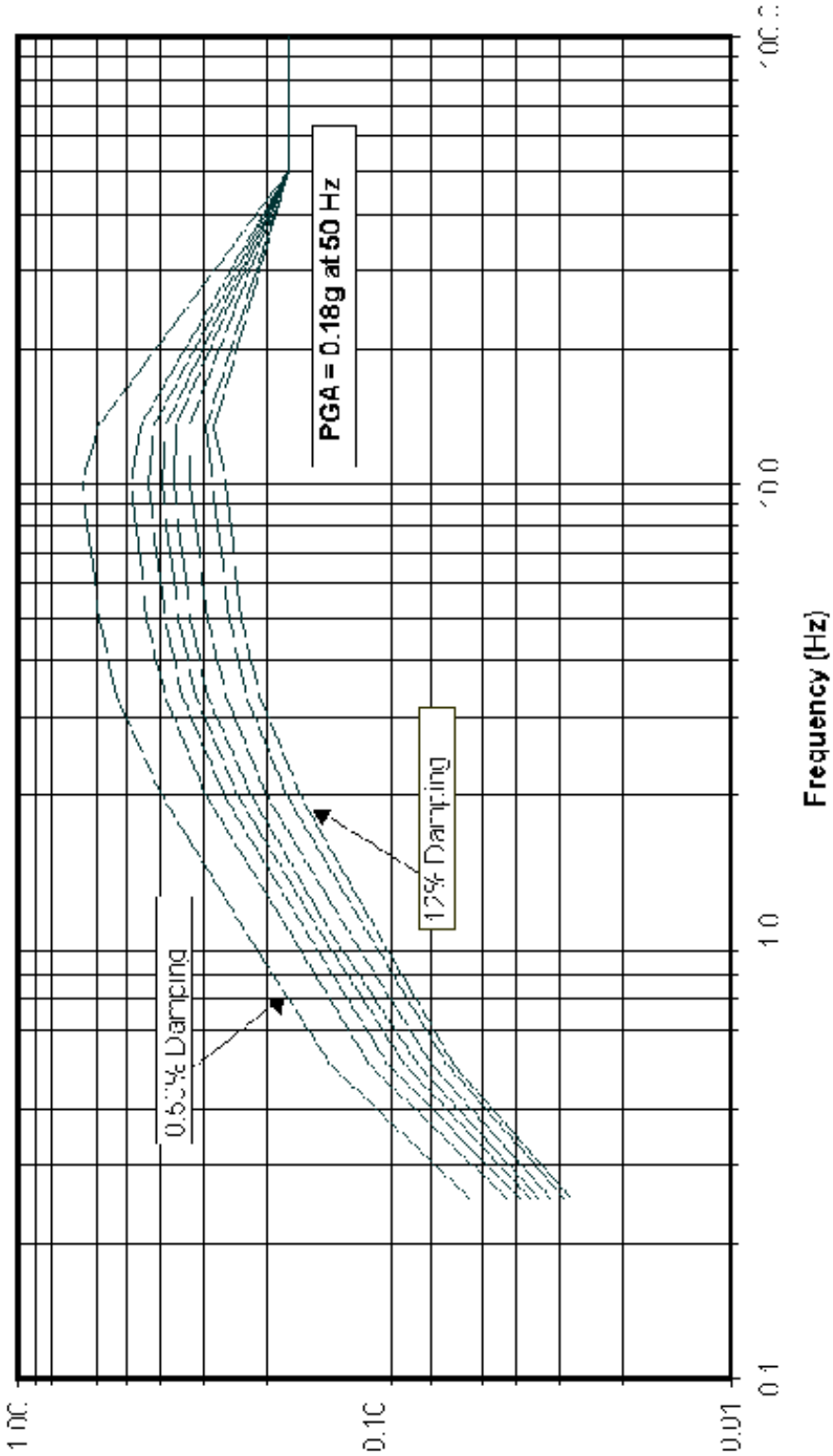


Figure 4-2

RPP-WTP DBE Vertical Response Spectra
(0.50%, 2%, 3%, 4%, 5%, 7%, 10%, 12% Damping)



Implementing Codes and Standards

ACI 349-97 Code Requirements for Nuclear Safety-Related Concrete Structures
ACI 349R-97 Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures
ANSI/AISC N690-94 Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities
ASCE 4-98 (Draft) Seismic Analysis of Safety-Related Nuclear Structures and Commentary
ASCE 7-95 Minimum Design Loads for Buildings and Other Structures
DOE-STD 1020-94 (Change 1, 1996) Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
1997 UBC Uniform Building Code
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.1 - 4

This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) without NPH safety functions.

SSCs that may be important to the safety of the RPP-WTP shall be designed to withstand the effects of NPH such as earthquakes, wind, and floods. The SSCs included under this criterion are:

1. SSCs Important to Safety (either Safety Design Class or Safety Design Significant) that do not have an NPH safety function,
2. SSCs that are not Important to Safety and that have significant inventories of radioactive or hazardous materials but in amounts less than quantities that might lead to an Important to Safety designation, and
3. SSCs that are important to safety because of their function to protect workers and members of the public from exposure to chemical hazards.

These SSCs are designated Seismic Category III (SC-III) for earthquakes and Performance Category 2 (PC-2) for other NPH.

SSCs included under this criterion shall be designed to withstand the NPH loadings as provided in Table 4-2.

Table 4-2. Natural Phenomena Design Loads for SSCs without NPH Safety Functions

Hazard	Load	Source Document for Load
Seismic	Uniform Building Code [a], Static Force Procedure	DOE-STD-1020-94 [b]
Straight wind	91 mi/hr 3-second gust, at 33 ft above ground, Importance factor, I=1.00	DOE Newsletter [c]
Wind Missile	Not Applicable	DOE-STD-1020-94 [b]
Tornado and Tornado Missiles	Not Applicable	DOE-STD-1020-94 [b]
Volcanic ash	5 lb/ft^2	HNF-SD-GN-ER-501 [d]
Flooding	Dry site for river flooding Local Precipitation: 2.5 in. for 6 hours	HNF-SD-GN-ER-501 [d]
Snow	15.0 lb/ft^2 snow load	HNF-SD-GN-ER-501 [d]

[a] 1997, *Uniform Building Code,* International Conference of Building Officials, Whittier, California.

[b] DOE STD-1020-94, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, U.S. Department of Energy, Washington, D.C., Change 1, 1996.

[c] DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98

[d] HNF-SD-GN-ER-501, Rev. 1, "Natural Phenomena Hazards, Hanford Site, South-Central Washington", Westinghouse Hanford Company

Implementing Codes and Standards

ACI 318-99 Building Code Requirements for Structural Concrete
ACI 318R-99 Commentary on Building Code Requirements for Structural Concrete
AISC MO16-89 Manual for Steel Construction - Allowable Stress Design, Ninth Edition
ASCE 7-95 Minimum Design Loads for Buildings and Other Structures
DOE-STD 1020-94 (Change 1, 1996) Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities
1997 UBC Uniform Building Code
ACI 530-95 Building Code Requirements for Masonry Structures and Commentary
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.1 - 5

Structures, systems, and components designated as Safety Design Class shall be appropriately protected against dynamic effects (e.g., the effects of missiles, pipe whipping, and discharging fluids) that may result from failures of moderate and high energy systems or other accident conditions.

In consideration of the need to protect structures, systems, and components which are designated as Safety Design Class from these dynamic effects, the failure of the moderate or high energy system need not be postulated to occur simultaneously with an accident unless the events are causally related.

Implementing Codes and Standards

ACI 349-97 Code Requirements for Nuclear Safety-Related Concrete Structures
ACI 349R-97 Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures
ANSI/AISC N690-94 Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities
ASCE 4-98 (Draft) Seismic Analysis of Safety-Related Nuclear Structures and Commentary
ASCE 7-95 Minimum Design Loads for Buildings and Other Structures
DOE-STD 1020-94 (Change 1, 1996) Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98

Safety Criterion: 4.1 - 6

Adequate provisions for facility security and physical protection of structures, systems, and components Important to Safety shall be provided.

Implementing Codes and Standards

PL-W375-MG0004, Safeguards and Security Program Plan

Regulatory Basis

DOE/RL-96-0006 4.3.6.1 Security-Security

4.2 Confinement Design

Safety Criterion: 4.2 - 1

The facility shall be designed to retain the radioactive and hazardous material through a conservatively designed confinement system for normal operations, anticipated operational occurrences, and accident conditions. The confinement system shall protect the worker and public from undue risk of releases such that the radiological and chemical exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2

Regulatory Basis

DOE/RL-96-0006 4.1.1.4 Defense in Depth-Mitigation

Safety Criterion: 4.2 - 2

Important to Safety liquid and gaseous systems and components, including pressure vessels, tanks, heat exchangers, piping, and valves, shall be designed to retain their hazardous inventory such that the radiological and chemical worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 4.2 - 3

Codes and standards for Important to Safety vessels and piping should be supplemented by additional measures (such as erosion/corrosion programs and piping in-service inspections) to mitigate conditions arising that could lead to a release of radiological or chemical material that would exceed the worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI)
Document P001/2 Rules for the Design of Piping Systems
Document V001/2 Rules for the Design of Vessels

Regulatory Basis

DOE/RL-96-0006 4.2.2.4 Proven Engineering Practices/Margins-Codes and Standards

Safety Criterion: 4.2 - 4

Liquid and gaseous storage systems designated as Important to Safety shall have continuous monitoring to detect the loss or degradation of their safe storage function. As appropriate the following shall be monitored:

1. temperature; pressure; radioactivity in ventilation exhaust and liquid effluent streams
2. liquid levels
3. tank chemistry; condensate and cooling water
4. generation of flammable and explosive mixtures of gases

Implementing Codes and Standards

ANSI N42.18-1980 (Rev 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S12.13 PT 1-95 Performance Requirements, Combustible Gas Detectors

4.3 Engineered Safety Systems

Safety Criterion: 4.3 - 1

Engineered safety systems shall be designed (1) to initiate automatically the operation of appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided.

Implementing Codes and Standards

ANSI/ANS 58.8-1994 Time Response Design Criteria for Safety-Related Operator Actions
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries

Regulatory Basis

DOE/RL-96-0006 *4.1.1.5 Defense in Depth-Automatic Systems*

Safety Criterion: 4.3 - 2

When single failure protection is required, Important to Safety engineered safety systems shall be designed to assure that the effects of natural phenomena (including lightning), and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
NFPA 780-95 Standard for the Installation of Lightning Protection Systems
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.3 - 3

Important to Safety engineered safety systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components Important to Safety resulting from a common-cause or common-mode failure.

The protection system shall be designed to permit periodic testing of its functioning when the facility is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006 4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure

Safety Criterion: 4.3 - 4

Important to Safety instrumentation and controls shall be provided to monitor variables and systems and control systems and components over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate public and worker safety by compliance to the standards of Safety Criteria 2.0-1 and 2.0-2, including those variables and systems that can affect the performance of Important to Safety facility conditions. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The instrumentation and controls provided shall provide the ability to detect off normal conditions, mitigate accidents, and place the facility in a safe state.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries

Regulatory Basis

DOE/RL-96-0006 4.1.1.3 Defense in Depth-Control
DOE/RL-96-0006 4.2.6.2 Human Factors-Instrumentation and Control Design

Safety Criterion: 4.3 - 5

When single failure protection is required, Important to Safety protection systems shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits

Safety Criterion: 4.3 - 6

The possibility of human error in facility operations shall be taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions and by providing means for detecting and correcting or compensating for error. The parameters to be monitored in control areas shall be selected and their displays arranged to ensure operators have clear and unambiguous indication of the status of the facility. The parameters and displays shall facilitate monitoring and the initiation and operation of systems designated as Important to Safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 1023-88 Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006	*4.1.1.6*	*Defense in Depth-Human Aspects*
DOE/RL-96-0006	*4.2.6.1*	*Human Factors-Human Error*
DOE/RL-96-0006	*4.2.6.2*	*Human Factors-Instrumentation and Control Design*
DOE/RL-96-0006	*4.2.6.3*	*Human Factors-Safety Status*

Safety Criterion: 4.3 - 7

The control room or control area shall be designed to permit occupancy and actions to be taken to monitor the facility safely during normal operations, and to provide safe control of the facility for anticipated operational occurrences and accident conditions. If credit is taken for operator action to satisfy the accident exposure standards of Safety Criteria 2.0-1 and/or 2.0-2, adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body gamma and 30 rem beta skin for the duration of the accident. For occurrences and accidents involving chemical release, provisions shall be made such that the operator exposure does not exceed the worker exposure standards of 29 CFR 1910.120 for emergency exposure.

Consideration shall also be given to accidents at nearby facilities if operator action is required to safely control the processes and bring them to a safe state.

The need for an alternate system that would allow the processes to be placed in a safe state in the event the primary control area is uninhabitable shall be evaluated.

Implementing Codes and Standards

ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
ASME N510-1989 (Rev 1995) Testing of Nuclear Air Cleaning Systems
NUREG-0800 Standard Review Plan, Section 6.4, Section II, Items 1-5.
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006	*4.2.4.1 Emergency Preparedness-Support Facilities*
DOE/RL-96-0006	*4.2.6.2 Human Factors-Instrumentation and Control Design*
29 CFR 1910.120	*Hazardous Waste Operations and Emergency Response*

4.4 Electrical and Mechanical Systems

Safety Criterion: 4.4 - 1

A list of electric and mechanical components designated as Important to Safety shall be prepared and maintained. The list shall include:

(1) The performance specifications for normal operation and under conditions existing during and following accidents.

(2) The load, pressure, voltage, frequency, and other characteristics, as appropriate, for which the performance specified can be ensured.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 4.4 - 2

Structures, systems, and components Important to Safety shall be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning shall be considered in design and qualification.

Implementing Codes and Standards

10 CFR 50.49 Environmental qualification of electric equipment important to safety for nuclear power
IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006 *4.2.2.3 Proven Engineering Practices/Margins-Safety System Design and Qualification*

Safety Criterion: 4.4 - 3

This Criterion has been deleted.

Safety Criterion: 4.4 - 4

Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.

Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin. Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended operating life.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI)

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006 4.2.7.1 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Reliability

DOE/RL-96-0006 4.2.7.2 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Availability, Maintainability, and Inspectability

Safety Criterion: 4.4 - 5

Each air treatment system designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and confinement capabilities to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) its safety function can be accomplished, assuming a single failure.

The use of alternate equipment may be considered to satisfy the single failure requirement.

Implementing Codes and Standards

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 6

Each air treatment system designated as Safety Design Class shall be designed to ensure its operability under normal and accident conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) the structural and leaktight integrity of its components

(2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves

(3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of associated systems

Implementing Codes and Standards

ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
UL 586-90 High Efficiency Particulate Air Filter Units, Seventh Edition

Safety Criterion: 4.4 - 7

Each air treatment system designated as Safety Design Significant shall be designed to ensure its operability under normal conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) the structural and leaktight integrity of its components

(2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves

(3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system

Implementing Codes and Standards

UL 586-90 High Efficiency Particulate Air Filter Units, Seventh Edition

Safety Criterion: 4.4 - 8

Ventilation systems and off-gas systems must be provided where necessary to control radiological and chemical material releases and the generation of flammable and explosive gases during normal and off-normal conditions.

Implementing Codes and Standards

ARI 670-90 Fans and Blowers
ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
ASME N510-1989 (Rev 1995) Testing of Nuclear Air Cleaning Systems
ASME PTC 11-84 Performance Test Codes, Fans
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 1002

Safety Criterion: 4.4 - 9

An onsite electric power system and an offsite electric power system shall be provided to permit functioning of systems designated as Safety Design Class. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure Safety Design Class functions are maintained in the event of postulated accidents. The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their specified safety functions assuming a single failure.

Implementing Codes and Standards

IEEE 308-91 Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 450-1995 Practice for Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Generating Stations and Substations
IEEE 484-1996 Recommended Practice for Installation Design and Installation of Large Lead Storage Batteries for Generating Stations and Substations
IEEE 485-1983 Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations
IEEE 628-1987 Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations
IEEE 741-1990 Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations
IEEE 946-1992 Design of Safety-Related DC Auxiliary Power Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 10

Physical and electrical separation shall be provided between diverse or redundant Safety Design Class electrical systems. Associated circuits should be avoided.

Implementing Codes and Standards

IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 628-1987 Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 11

Electric power systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to periodically test:

(1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses

(2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of the offsite power system and the onsite power system

Implementing Codes and Standards

IEEE 338-1987 Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 12

Electric power systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to periodically test:

(1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses

(2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 387-1995 Standard Criteria for Diesel-Generator Units Applied as Standby Power Generating Stations
NFPA 70-1996 National Electric Code

Safety Criterion: 4.4 - 13

Instrument air systems designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 14

Instrument air systems designated as Safety Design Class that provide air to a non-Safety Design Class air system shall be provided with adequate isolation such that failure of the non-Safety Design Class portion of the system will not prevent the Safety Design Class portion from performing its specified safety function.

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems

Safety Criterion: 4.4 - 15

Instrument air systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic pressure and functional testing to assure:

(1) air quality

(2) the structural integrity of its components

(3) the operability and the performance of the active components of the system

(4) the operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems
ASME B31.3-96 Process Piping
ASME PTC 9-70 Performance Test Codes, Displacement Compressors, Vacuum Pumps and Blowers
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 16

Instrument air systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic pressure and functional testing to assure:

(1) air quality

(2) the structural integrity of its components

(3) the operability and the performance of the active components of the system

(4) the operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME PTC 9-70 Performance Test Codes, Displacement Compressors, Vacuum Pumps and Blowers
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
ISA S7.0.01-1996 Quality Standard for Instrument Air

Safety Criterion: 4.4 - 17

Instrument air systems supplying air to Important to Safety equipment shall provide clean, dry, and oil free air to this equipment. The instrument air shall be free of all corrosive and hazardous gases which may be drawn into the system.

Implementing Codes and Standards

ISA S7.0.01-1996 Quality Standard for Instrument Air

Safety Criterion: 4.4 - 18

Cooling water systems designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

Implementing Codes and Standards

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 19

Cooling water systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) Long term corrosion and/or organic fouling that could degrade system performance is detected. This shall include consideration of the impacts of organic fouling on heat exchanger performance.

(2) The potential for radioactive leakage into and out of the system and to the environment is minimized.

(3) The structural and leaktight integrity of its components.

(4) The operability and the performance of the active components of the system.

(5) The operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 20

Cooling water systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) Long term corrosion and/or organic fouling that could degrade system performance is detected. This shall include consideration of the impacts of organic fouling on heat exchanger performance.

(2) The potential for radioactive leakage into and out of the system and to the environment is minimized.

(3) The structural and leaktight integrity of its components.

(4) The operability and the performance of the active components of the system.

(5) The operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
NFPA 214-96 Standard on Water-Cooling Towers
TEMA B, C, or R TEMA Class “B”, “C”, or “R” Heat Exchangers Mechanical Standards

Safety Criterion: 4.4 - 21

Safety Design Class motor operated valves shall be specified to ensure operability against the maximum differential pressure that might occur while performing their specified accident prevention or mitigation safety function at the minimum specified terminal voltage. Consideration for mis-positioned valves is not a requirement in determining the maximum differential pressure.

Periodic testing of Safety Design Class motor operated valves shall be performed to confirm their ability to perform their specified accident prevention or mitigation safety function.

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 382-1985 Standard for Qualification of Actuators for Power Operated Valve Assemblies with Safety-Related Functions for Nuclear Power Plants

4.5 Fire Protection

Safety Criterion: 4.5 - 1

Two reliable and separate water supplies of adequate capacity for fire suppression shall be provided.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 2

Buildings containing a significant quantity of radioactive and/or hazardous material shall be constructed of noncombustible or fire-resistive material, where appropriate.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 3

Confinement of the fire to its origin should be achieved through passive barriers and by activating systems such as fire and smoke dampers, exhaust fans, and drainage pumps to prevent migration of gases, hot combustion products, and flammable liquids outside the fire area.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 4

Automatic fire extinguishing systems shall be included in all areas subject to loss of Safety Design Class systems, significant life safety hazards, or unacceptable program interruption, unless the Fire Hazards Analysis dictates otherwise.

As determined by the Fire Hazards Analysis special hazards shall be provided with additional fixed protection systems.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 5

Redundant Safety Design Class systems and components should be in separate fire areas.

Redundant, primary and secondary, fire protection systems shall be provided in areas where Safety Design Class systems and components are vulnerable to fire damage and where no redundant safety capability exists outside of the fire area.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 6

The design shall incorporate life safety features including means to notify and evacuate building occupants in the event of a fire, such as a fire detection or fire alarm system and illuminated, protected egress paths.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 7

The facility shall include a fire detection system to detect the presence of a fire and activate alarm systems so that measures for confinement and suppression of the fire and personnel evacuation may start promptly. The detection system shall include a means to summon the Hanford Site fire department. The system shall be capable of operation without offsite power.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 8

The facility shall include physical access and appropriate equipment to facilitate effective intervention by the Hanford Site fire department, such as an interior standpipe system.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 9

The facility design shall provide for the prevention of accidental release of significant quantities of contaminated products of combustion and fire fighting water to the environment. This can be provided by such features as ventilation control and filter systems, curbs, dikes, and holding ponds.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 10

Fire and related hazards that are unique to the facility and are not addressed by industry codes and standards shall be protected by isolation, segregation, or use of special fire control systems, such as inert gas or explosion suppression, as determined by the Fire Hazards Analysis.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 11

Fire protection systems shall be designed, and/or systems and components protected, such that its/their inadvertent operation, inactivation, or failure of structural stability will not result in the loss of a Safety Design Class function.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 12

The fire protection program shall establish the fire protection policy for the protection of the facility and the procedures, equipment, and personnel required to implement the program. The program shall have the following objectives:

(1) To prevent fires from starting

(2) To detect early, control and extinguish promptly those fires that do occur

(3) To provide protection for Safety Design Class SSCs

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 13

The fire protection program and features shall be characterized by a level of fire protection that is sufficient to fulfill the requirements of the best protected class of industrial risks ("Highly Protected Risk" or "Improved Risk") and shall be provided protection to achieve "defense-in-depth."

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 14

A fire protection program shall be developed that will minimize the potential for the occurrence of a fire or explosive threat and, should such an event occur, the program will limit:

(1) Radiological and hazardous releases from the facility

(2) The threat to the health and safety of facility workers

(3) Interruption of the facility mission to process tank waste

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 15

The fire protection program will include:

(1) organization, training, and responsibilities of the fire protection staff, including a trained and equipped emergency services organization

(2) inspection, testing, and maintenance of all fire protection systems by personnel properly qualified by experience and training in fire protection systems

(3) surveillance to ensure that fire barriers are in place and that fire suppression systems and components are operable

(4) training of all employees in basic fire safety

(5) periodic performance of fire drills

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 16

The fire protection program will include a plan to identify, prioritize, and monitor the status of fire protection-related appraisal findings/recommendations until final resolution is achieved. When final resolution will be significantly delayed, appropriate interim compensatory measures shall be implemented to minimize the fire risk.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 17

The fire protection program shall ensure fire protection requirements are documented and incorporated in the plans and specifications for all new facilities and for significant modifications of existing facilities. This includes a documented review by a qualified fire protection engineer of plans, specifications, procedures, and acceptance tests.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 18

The fire protection program shall include a comprehensive, documented fire protection self-assessment program, which includes all aspects (program and facility) of the fire protection program.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 19

Administrative controls shall be established to minimize fire hazards. These shall include procedures to:

(1) govern the handling and storage of combustible and flammable materials

(2) govern the handling of transient fire loads in buildings containing Safety Design Class SSCs

(3) designate staff members responsible for fire protection review of proposed work activities

(4) govern the use of ignition sources (e.g., through the use of a flame permit system)

(5) control the expedient removal of combustibles resulting from work activities

(6) establish compensatory controls for activities which may result in the impairment of fire prevention and/or mitigation features

(7) maintain periodic housekeeping inspections to ensure continued compliance with these administrative controls

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 20

A Fire Hazard Analysis (FHA) of the facility shall be performed. Such a systematic analysis shall divide the facility into "fire areas" and evaluate the fire safety of each area and of the facility as a whole. The analysis shall, for each fire area:

(1) Account for all radioactive, hazardous, and combustible materials, including estimates of their heat content

(2) Describe the processes performed and their potential for fire or explosion

(3) Account for the sources of heat and flame

(4) List the fire detection and suppression equipment

(5) Consider credible fire scenarios and evaluate the adequacy of the fire protection measures

In addition, the FHA shall consider other buildings or installations close to process buildings that contain flammable, combustible, or reactive liquid or gas storage.

The FHA shall confirm that the facility can be placed in a safe state during and after all credible fire and explosion conditions.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 21

The fire protection program shall be under the direction of an individual who has been delegated authority commensurate with the responsibilities of the position and who has available staff knowledgeable in both fire protection and nuclear safety.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 22

The facility should have on file, and ready to use, a Pre-Fire Plan. The Pre-Fire Plan should assign individual and alternate responsibilities for responding to a fire alarm or call; assessing the situation, suppressing incipient fires, assembling the emergency service organization, personnel evacuation, orderly shutdown of processes, and safeguarding (if necessary) and control of radioactive and hazardous material.

The plan should clearly indicate, preferably with the help of site plans and drawings, the locations of the fire department-compatible connections and fire-fighting equipment, such as portable extinguishers, automatic fire suppression systems, sectional valves, standpipes, hydrants, and hoses. It should also indicate the areas of concentrations of combustibles, storage of flammable and combustible liquids, and areas where use of water for fire suppression is restricted because of nuclear criticality or other concerns.

The Pre-Fire Plan should be prepared in consultation and coordination with the Hanford Site fire department. The Hanford Site fire department personnel should be given familiarization tours of the facility at least once a year.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 23

Hot work permits shall be issued for hot work operations conducted in or near the facility. The permit shall document that applicable fire prevention and protection requirements have been implemented prior to beginning the hot work operations; it shall indicate the date(s) authorized for hot work; and identify the object on which hot work is to be performed. The permit shall be kept on file until completion of the hot work operations.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Regulatory Basis

DOE/RL-96-0006 5.2.8 Hot Work Control

5.0 Radiation Protection

Safety Criterion: 5.0 - 1

A Radiation Protection Program (RPP) compliant with 10 CFR 835 shall be developed and submitted for approval to DOE.

The RPP-WTP Radiological Controls Program shall address all items in 10 CFR 835 and the additional Safety Criteria provided in SRD Volume II Sections 5.1 and 5.2.

Implementing Codes and Standards

DOE G 441.1-1, Management and Administration of Radiation Protection Programs Guide

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 101(a-f)
DOE/RL-96-0006 4.2.3.1 Radiation Protection-Radiation Protection Practices
DOE/RL-96-0006 4.3.2.1 Radiation Protection-Radiation Practices
DOE/RL-96-0006 4.3.2.2 Radiation Protection-Procedures and Monitoring

5.1 Occupational Radiation Protection

Safety Criterion: 5.1 - 1

This safety criterion has been deleted.

Safety Criterion: 5.1 - 2

A respiratory protection program shall be established that includes:

(1) Use of respiratory protection equipment, including equipment used as emergency devices, that is tested and certified or had certification extended by the National Institute for Occupational Safety and Health/Mine Safety and Health Administration (NIOSH/MSHA).

(2) Air sampling sufficient to identify the potential hazard, permit proper equipment selection, and estimate exposures.

(3) Surveys and bioassays, as appropriate, to evaluate actual intakes.

(4) Testing of respirators for operability immediately prior to each use.

(5) Written procedures regarding selection, fitting, issuance, maintenance, and testing of respirators, including testing for operability immediately prior to each use; supervision and training of personnel; monitoring, including air sampling and bioassays; and recordkeeping.

(6) Determination by a physician prior to the initial fitting of respirators, and either every 12 months thereafter or periodically at a frequency determined by a physician, that the individual user is medically fit to use the respiratory protection equipment.

(7) A written policy statement on respirator usage covering:

(i) The use of process or other engineering controls, instead of respirators.

(ii) The routine, nonroutine, and emergency use of respirators.

(iii) The periods of respirator use and relief from respirator use. Each respirator user will be informed that they may leave the area at any time for relief from respirator use in the event of equipment malfunction, physical or psychological distress, procedural or communication failure, significant deterioration of operating conditions, or any other conditions that might require such relief.

(8) Use of equipment within limitations for type and mode of use and provision for proper visual, communication, and other special capabilities (such as adequate skin protection) when needed.

(9) Notification to the Regulator, in writing, at least 30 days before the date that respiratory protection equipment is first used to protect workers from airborne radioactivity.

Implementing Codes and Standards

ANSI Z-88.2-1992 American National Standard for Respiratory Protection

Safety Criterion: 5.1 - 3
This safety criterion has been deleted.

Safety Criterion: 5.1 - 4
This safety criterion has been deleted.

Safety Criterion: 5.1 - 5
This safety criterion has been deleted.

Safety Criterion: 5.1 - 6
This safety criterion has been deleted.

Safety Criterion: 5.1 - 7
This safety criterion has been deleted.

5.2 Occupational Radiation Protection Design

Safety Criterion: 5.2 - 1

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 2

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 3

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 4

This Safety Criterion has been deleted

5.3 Environmental Radiation Protection

Safety Criterion: 5.3 - 1

An Environmental Radiological Protection Program shall be prepared and submitted to the regulator.

The Environmental Radiological Protection Program (ERPP) shall address the following elements, as appropriate:

(1) the identity of existing and anticipated types of activities and areas of the site subject to the ERPP

(2) the measures to be used to implement the ERPP

(3) the methods to be used to monitor, report, and record compliance with the ERPP

(4) models and methods used for dose assessment including bioaccumulation and dose-conversion factors

(5) an As Low As is Reasonably Achievable (ALARA) Program

(6) effluent and environmental monitoring including:

- (i) sources of airborne emissions
- (ii) sources of discharges in liquid waste streams
- (iii) effluent monitoring
- (iv) environmental surveillance
- (v) meteorological data acquisition
- (vi) pre-operational evaluation

(7) ground water protection

(8) radiological protection in the management of radioactive waste

(9) controls on the release of materials

(10) property containing residual radioactive materials

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specifications with guidance for use

Regulatory Basis

DE-AC06-96RL13308 Part I Section C.5 Table S4-1
DOE/RL-96-0006 4.3.2.1 Radiation Protection-Radiation Practices
DOE/RL-96-0006 4.3.2.2 Radiation Protection-Procedures and Monitoring

Safety Criterion: 5.3 - 2

The ALARA Program shall ensure that releases of radioactive materials to the environment and exposures to the public during normal operations shall be kept ALARA and within prescribed limits.

Implementing Codes and Standards

DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features
WAC 173-480 Ambient Air Quality Standards and Emission Limits for Radionuclides Location: Part 050 (1)

Safety Criterion: 5.3 - 3

A waste management program shall ensure compliance with all applicable laws and regulations. The waste management program shall also ensure that the radiological impact to the general public and environment due to radioactive wastes arising from RPP-WTP operation shall be ALARA.

Implementing Codes and Standards

IAEA Safety Series No. 50-SG-011, Operational Management for Radioactive Effluents and Wastes Arising in Nuclear Power Plants.
ANSI/ISO-14001-1996, Environmental Management Systems - Specifications with guidance for use

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features

Safety Criterion: 5.3 - 4

Equipment shall be designed and installed to monitor and maintain control over radioactive materials in gaseous and liquid effluents produced during normal operations, including anticipated operational occurrences.

Implementing Codes and Standards

40 CFR 52 Appendix E Performance Specifications and Specification Test Procedures for Monitoring Systems for Effluent Stream Gas Volumetric Flow Rate
40 CFR 60 Appendix A, Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17
ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N42.18-1980 (R 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
ANSI N323 Radiation Protection Instrumentation Test and Calibration
ASME/ANSI AG-1, Code on Nuclear Air and Gas Treatment
ASME/ANSI N509, Nuclear Power Plant Air-Cleaning Units and Components
ASME/ANSI N510, Testing of Nuclear Air Cleaning Systems
ACGIH 1988, Industrial Ventilation, A Manual of Recommended Practice, 20th Edition, American Conference of Governmental Industrial Hygienists.
ERDA 76-21, Nuclear Air Cleaning Handbook

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075
WAC 246-247 Radiation Protection - Air Emissions Location: Part 110

Safety Criterion: 5.3 - 5

All new construction and significant modifications of air emission units shall utilize best available radionuclide control technology (BARCT).

Implementing Codes and Standards

WAC 246-247-120 Appendix B BARCT Compliance Demonstration
ASME/ANSI AG-1, Code on Nuclear Air and Gas Treatment
ASME/ANSI N509, Nuclear Power Plant Air-Cleaning Units and Components
ASME/ANSI N510, Testing of Nuclear Air Cleaning Systems
ANSI N13.1, Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N42.18, Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
ERDA 76-21, Nuclear Air Cleaning Handbook
ACGIH 1988, Industrial Ventilation, A Manual of Recommended Practice, 20th Edition, American Conference of Governmental Industrial Hygienists.
40 CFR 60 Appendix A, Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17

Regulatory Basis

WAC 173-480 Ambient Air Quality Standards and Emission Limits for Radionuclides Location: Part 060
WAC 246-247 Radiation Protection - Air Emissions Location: Part 040 (3)

Safety Criterion: 5.3 - 6

Activities shall be conducted in such a manner that no radioactive material is discharged into sanitary sewers. Exempt from this Safety Criterion are trace radioactive materials present in:

(1) readily soluble waste such as kitchen waste from breakrooms, custodial cleaning solutions, or other materials of similar non-RPP-WTP process origin

(2) biological waste (solid and liquid human waste) which is readily dispersed in water

Also exempt from this Safety Criterion are excreta from individuals undergoing medical diagnosis or therapy with radioactive materials.

Implementing Codes and Standards

IAEA Safety Series No. 50-SG-011, Operational Management for Radioactive Effluents and Wastes Arising in Nuclear Power Plants.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.2*	*Radiation Protection-Radiation Protection Features*

Safety Criterion: 5.3 - 7

Liquid discharges from the facility, other than sanitary sewer discharges, shall comply with ALARA process requirements, be treated by the best available technology, and not result in release of settleable solids to surface waters for streams exceeding 5 pCi/g for alpha-emitting radionuclides, and/or 50 pCi/g for beta-emitting radionuclides.

Note: The RPP-WTP design does not include provisions for liquid waste discharges, other than sanitary sewer discharges. Therefore, Implementing Codes and Standards are not required. If the RPP-WTP design changes such that liquid discharges result, an SRD revision will be prepared.

Safety Criterion: 5.3 - 8

Controls on the release of materials and property containing residual radioactive material shall be established.

Implementing Codes and Standards

10 CFR 835, Occupational Radiation Protection, Appendix D (ad hoc)

Note: The Appendix D values will be used as surface contamination criteria for determining the suitability of releasing material from radiologically controlled areas. These criteria are not applicable to materials potentially contaminated throughout their volume. Because the RPP-WTP process feed is a mixed waste, any items that are determined to be contaminated, will also be assumed to be a mixed waste (i.e., containing a State of Washington dangerous waste). Rather than determine the quantities of dangerous wastes present, these materials will be disposed of as mixed wastes.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.1*	*Radiation Protection-Radiation Protection Practices*

5.4 Environmental Radiological Monitoring

Safety Criterion: 5.4 - 1

Each source shall have capability for independent effluent emission testing as follows:

(1) Sampling ports adequate for test methods applicable to each source

(2) Safe sampling platform(s)

(3) Safe access to sampling platform(s)

(4) Utilities for sampling and testing equipment

(5) Any other facilities deemed necessary to safely and properly test a source

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 13
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (10)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (9)

Safety Criterion: 5.4 - 2

Nonpoint and fugitive emissions of radioactive material shall be monitored.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (8)

Safety Criterion: 5.4 - 3

Direct measurements shall be made, to the extent practicable, to obtain information characterizing source terms, exposures, exposure modes, and other information needed in evaluating doses.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

WAC 246-221 Radiation Protection Standards Location: 070 (1)

Safety Criterion: 5.4 - 4

When the effluents from a single source, or from two or more sources subject to the same emission standards, are combined before being released to the atmosphere, a monitoring system shall be installed on each effluent or on the combined effluent. If two or more sources are not subject to the same emission standards, a separate monitoring system shall be installed on each effluent. If the applicable standard is a mass emission standard and the effluent from one source is released to the atmosphere through more than one point, a monitoring system shall be installed at each emission point.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 14 (d)

Safety Criterion: 5.4 - 5

Equipment and procedures used for the continuous monitoring of radioactive air emissions shall conform, to applicable guidance.

Implementing Codes and Standards

40 CFR 52 Appendix E Performance Specifications and Specification Test Procedures for Monitoring Systems for Effluent Stream Gas Volumetric Flow Rate
40 CFR 60 Appendix A, Test Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17
40 CFR 61 Appendix B, Test Method 114
ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N323 Radiation Protection Instrumentation Test and Calibration
ANSI N42.18-1980 (R 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (2)

Safety Criterion: 5.4 - 6

Computer codes or procedures used to determine the offsite total effective dose equivalent from airborne emissions shall be EPA approved.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (2)

Safety Criterion: 5.4 - 7

Compliance with the annual dose limit for individual members of the public (100 mrem/yr from all sources) shall be shown by:

(1) Demonstrating by measurement or calculation that the total effective dose equivalent to the individual likely to receive the highest dose from the operation does not exceed the annual dose limit; or

(2) Demonstrating that:

(a) The annual average concentrations of radioactive material released in gaseous and liquid effluents at the boundary of the unrestricted area do not exceed the values specified in Table II of WAC246-221-290.

(b) If an individual were continuously present in an unrestricted area, the dose from external sources would not exceed 0.002 rem in an hour and 0.05 rem in a year.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-221 Radiation Protection Standards Location: 070 (2)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (1)

Safety Criterion: 5.4 - 8

Compliance with the public air emission standard shall be determined by calculating the highest effective dose equivalent to any member of the public at any offsite point where there is a residence, school, business or office.

The determination of compliance shall include all radioactive air emissions resulting from routine and nonroutine operations for the past calendar year.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 94
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (3)

Safety Criterion: 5.4 - 9

Records sufficient to demonstrate compliance with the dose limit for individual members of the public shall be maintained. Records must document the source of input parameters including the results of all measurements upon which they are based, the calculations and/or analytical methods used to derive values for input parameters, and the procedure used to determine compliance. This documentation should be sufficient to allow an independent auditor to verify the accuracy of the determination made concerning the facility's compliance.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 95
WAC 246-247 Radiation Protection - Air Emissions Location: Part 080

Safety Criterion: 5.4 - 10

An environmental surveillance program shall be developed and implemented to include:

(1) Meteorological data acquisition (Note 1)

(2) Pre-operational evaluation (Note 2)

(3) Near-Facility Monitoring (Note 3)

(4) Ground Water Protection (Note 4)

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with guidance for use

IAEA Safety Series No 41, *Objectives and Design of Environmental Monitoring Programmes for Radioactive Contaminants*

Notes:

1. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-22 between DOE and BNFL Inc. for Air Emissions,* Table 2 states that DOE will maintain the Hanford Site Air Operating Permit (AOP) and provide access to meteorological data.
2. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-09 Between DOE and BNFL Inc. for Land Siting,* Table 1, describes specific interfaces responsibilities for the RPP-WTP contractor and for the DOE. Item 12 of the table requires that the RPP-WTP contractor perform any additional site characterization work beyond that which was performed by the DOE. The RPP describes the plans and measures for compliance with the survey and contamination control requirements of 10 CFR 835.
3. As described in BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-22 between DOE and BNFL Inc. for Air Emissions,* DOE will continue to operate site and near-facility monitoring networks in the vicinity of the RPP-WTP site. Additional monitoring which is required will be provided by the RPP-WTP contractor. If additional monitoring is required, it will be performed consistent with the Hanford Site near-facility monitoring program for inclusion in site annual reports (example, HNF-EP-0573-6, *Hanford site Near-Facility Environmental Monitoring Annual Report, Calendar Year 1997*).
4. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-09 between DOE and BNFL Inc. for Land Siting,* Section 3.3, Ground Water Monitoring Wells, states that that the DOE will "…close groundwater monitoring well E25-32 prior to the start of site work…" There is no liquid discharge to the environment from RPP-WTP operations. Transfer piping to the Effluent Treatment Facility is by means of a three-inch pipe encased in a 6-inch pipe. Potential leakage from the transfer pipe is contained, and collected by the outer pipe. Accidental release of the inner pipe contents would be detected by the transfer pipe leak detection equipment. If both inner and outer pipes failed, such leakage could result in soil contamination which would be remediated prior to any contamination reaching the ground water.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.1*	*Radiation Protection-Radiation Protection Practices*

6.0 Startup

Safety Criterion: 6.0 - 1

A pre-operational testing program shall be established and followed to demonstrate that Important to Safety structures, systems and components have been properly constructed and can perform their specified functions. The program shall provide for the detection, tracking, and correction of deficiencies.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.1 Pre-Operational Testing-Testing Program

Safety Criterion: 6.0 - 2

Procedures for normal facility and systems operation and for functional tests to be performed during the operating phase shall be validated as part of the pre-operational testing program.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.2 Pre-Operational Testing-Operational Systems and Functional Testing Procedures Validation

Safety Criterion: 6.0 - 3

During pre-operational testing, detailed diagnostic data shall be collected on systems and components designated as Important to Safety and the initial operating parameters of the systems and components shall be recorded.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.3 Pre-Operational Testing-Safety Systems Data

Safety Criterion: 6.0 - 4

During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components designated as Important to Safety shall be determined and documented. Operating points shall be adjusted to conform to values in the design basis. Training procedures and limiting conditions for operation shall be modified, if necessary, to accurately reflect the operating characteristics of the systems and components as built.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 3.14 Startup Testing and Operation
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.4 Pre-Operational Testing-Design Operating Characteristics

Safety Criterion: 6.0 - 5

A pre-startup safety review shall be performed. The pre-startup safety review shall confirm that, prior to the introduction of radioactive or process chemicals considered to pose a hazard to a process, construction and equipment is in accordance with design specifications; safety, operating, maintenance, and emergency procedures are in place and are adequate; a process hazard analysis has been performed and recommendations have been resolved or implemented before startup; and training of each employee involved in operating a process has been completed.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.3.1.4 Conduct of Operations-Readiness
DOE/RL-96-0006 5.2.6 Pre-startup Safety Review

7.0 Management and Operations

Safety Criterion: 7.0 - 1

Normal operations shall be conducted in accordance with approved operational safety requirements and in strict accordance with administrative and procedural controls.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.13 Procedures
Section: 5.6.1 Procedure Development

Regulatory Basis

DOE/RL-96-0006 4.3.1.2 Conduct of Operations-Normal Operations
DOE/RL-96-0006 5.1.3 Process Safety Responsibility

Safety Criterion: 7.0 - 2

Normal operation, including anticipated operational occurrences, maintenance, and testing, shall be controlled so that facility and system variables remain within their normal operating ranges and the frequency of demands placed on Important to Safety structures, systems, and components are small.

Implementing Codes and Standards

Regulatory Basis

DOE/RL-96-0006 4.1.1.3 Defense in Depth-Control

Safety Criterion: 7.0 - 3

The operating organizations shall become and remain familiar with the features and limitations of components included in the design of the facility. They shall obtain appropriate input from the design organization on pre-operational testing, operating procedures, and the planning and conduct of training.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 1.3.15 Operations

Regulatory Basis

DOE/RL-96-0006 4.1.5.2 Configuration Management-Contractor Design Knowledge

Safety Criterion: 7.0 - 4

The assignment and subdivision of responsibility for safety within the contractor's organization shall be kept well defined throughout the life of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.2 Safety Responsibilities
Section: 6.1.2 Lines of Authority and Responsibility

Regulatory Basis

DOE/RL-96-0006	*4.1.2.2*	*Safety Responsibility-Safety Assignments*
DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*

7.1 Management and Organization/Staffing

Safety Criterion: 7.1 - 1

Safety management shall oversee the implementation of the risk management program elements. A qualified person shall be assigned the overall responsibility for the development, implementation, and integration of the risk management program elements. If responsibility for implementing individual requirements of the risk management program is assigned to other persons, the names or positions of these people shall be documented and the lines of authority defined through an organization chart or similar document.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 6.1 Integration into Work Planning and Performance

Regulatory Basis

Safety Criterion: 7.1 - 2

When selecting a subcontractor, information regarding the subcontract employer's safety performance and programs shall be obtained and evaluated. Subcontract employees shall be informed of the known potential fire, explosion, or toxic release hazards related to the subcontractor's work and the process. The applicable provisions of the emergency plan shall be explained to the subcontractors. Safe work practices to control the entrance, presence, and exit of subcontract employers and employees in radioactive or hazardous process areas shall be developed and implemented. The performance of subcontract employers with regard to safety shall be periodically evaluated and a subcontract employee injury and illness log related to the subcontractor's work in process areas shall be maintained.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.2 Control of Subcontractors

Regulatory Basis

DOE/RL-96-0006 5.2.5 Subcontractors

Safety Criterion: 7.1 - 3

A framework shall be established for safety review organizations that are responsible for assuring the safety of the facility. The separation between the responsibilities of the safety review organizations and those of the other organizations shall remain clear so that the safety review organizations retain their independence as safety authorities. Internal safety oversight should be conducted by qualified personnel to ensure that the safety standards are consistently met.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.13 Procedures
- Section: 3.16 Internal Safety Oversight
- Chapter: 10.0 Assessments

Regulatory Basis

DOE/RL-96-0006	*4.1.4.1*	*Safety/Quality Culture-Safety/Quality Culture*
DOE/RL-96-0006	*4.3.1.5*	*Conduct of Operations-Internal Surveillance and Audits*
DOE/RL-96-0006	*4.4.1*	*Safety Review Organization*
DOE/RL-96-0006	*4.4.2*	*Qualified Personnel*
DOE/RL-96-0006	*5.1.3*	*Process Safety Responsibility*

Safety Criterion: 7.1 - 4

Commitments from outside organizations to provide data and services required to satisfy safety obligations shall be made prior to the need for the information or services.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.18 Emergency Planning
- Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006	*4.1.2.3*	*Safety Responsibility-Site and Technical Support*

7.2 Training and Procedures

Safety Criterion: 7.2 - 1

Programs providing for continual training and qualification for operations, maintenance, and technical support personnel, to enable them to perform their duties safely and efficiently, shall be developed and implemented utilizing a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.12 Training
Section: 3.15 Training and Qualification
Section: 4.2.2 Training and Procedures

Regulatory Basis

DOE/RL-96-0006	*4.3.1.7*	*Conduct of Operations-Access to Technical Safety Support*
DOE/RL-96-0006	*4.3.4.2*	*Training and Qualifications-Training Programs*

Safety Criterion: 7.2 - 2

A training program must be established, implemented, and maintained for individuals relied upon to operate, maintain, or modify the facility in a safe manner. The training program shall be based on a systems approach to training that includes the following:

(a) Systematic analysis of the jobs to be performed

(b) Learning objectives derived from the analysis which describe desired performance after training

(c) Training design and implementation based on the learning objectives

(d) Evaluation of trainee mastery of the objectives during training

(e) Evaluation and revision of the training based on the performance of trained personnel in the job setting

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification

Safety Criterion: 7.2 - 3

Each employee involved in operating a process shall be trained in an overview of the process and in the operating procedures/instructions. The training shall include emphasis on the specific safety and health hazards, operating limits, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.

Refresher training shall be provided at least every three years, and more often if necessary, to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures/instructions of the process and is proficient in the procedures to follow if conditions exceed the design basis of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.3 Development of the Operator Training Program

Regulatory Basis

DOE/RL-96-0006 4.3.4.1 Training and Qualifications-Personnel Training
DOE/RL-96-0006 4.3.4.3 Training and Qualifications-Conditions Beyond Design Basis
DOE/RL-96-0006 5.2.4 Training
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

Safety Criterion: 7.2 - 4

Up-to-date records of training status shall be maintained which contain the names of the trained employees, the types of training, the dates of training, and the means used to verify that the employees understood the training.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

Safety Criterion: 7.2 - 5

Written procedures/instructions that provide clear direction for safely conducting activities involving radioactive or hazardous materials shall be developed and implemented for each phase of the facility life. The procedures/instructions shall address at least the following elements:

(1) Steps for each operating phase:
   - (a) Initial startup
   - (b) Normal operations
   - (c) Temporary operations
   - (d) Emergency shutdown including the conditions under which emergency shutdown is required, and the assignment of shutdown responsibility to qualified operators to ensure that emergency shutdown is executed in a safe and timely manner
   - (e) Emergency operations
   - (f) Normal shutdown
   - (g) Startup following a turnaround, or after an emergency shutdown

(2) Operating limits:
   - (a) Consequences of deviation
   - (b) Steps required to correct or avoid deviation

(3) Safety and health considerations:
   - (a) Properties of, and hazards presented by, the chemicals used in the process
   - (b) Precautions necessary to prevent exposure, including engineering controls, administrative controls, and personal protective equipment
   - (c) Control measures to be taken if physical contact or airborne exposure occurs
   - (d) Quality control for raw materials and control of hazardous chemical inventory levels
   - (e) Any special or unique hazards

(4) Safety systems and their functions

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.1 Procedure Development

Regulatory Basis

DOE/RL-96-0006	*4.3.2.2*	*Radiation Protection-Procedures and Monitoring*
DOE/RL-96-0006	*5.2.3*	*Operating Procedures*

Safety Criterion: 7.2 - 6

Operating procedures shall be readily accessible to employees who work in or maintain a process with radioactive or hazardous materials.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.1 Procedure Development

Regulatory Basis

Safety Criterion: 7.2 - 7

Operating procedures shall be reviewed as often as necessary to assure that they reflect current operating practice, including changes that result from changes in process chemicals, technology, and equipment, and changes to facilities. These procedures shall be certified annually that they are current and accurate.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.3 Configuration Management
Section: 5.6.1 Procedure Development

Regulatory Basis

Safety Criterion: 7.2 - 8

Safe work practices providing for the control of hazards during operations such as lockout/tagout; confined space entry; opening process equipment or piping; and control over entrance into a facility by maintenance, subcontractor, laboratory, or other support personnel shall be developed. These safe work practices shall apply to employees and subcontractor employees.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.4 Safety/Quality Culture
Section: 5.2 Control of Subcontractors
Section: 5.6.6 Hot Work Operations

Regulatory Basis

7.3 Quality Assurance Program

Safety Criterion: 7.3 - 1

The following quality assurance elements shall be applied using a graded approach:

(1) Quality Assurance Program
(2) Personnel Training and Qualification
(3) Quality Improvement
(4) Documents and Records
(5) Work Processes
(6) Design
(7) Procurement
(8) Inspection and Acceptance Testing
(9) Management Assessment
(10) Independent Assessment.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.11 Quality Levels

Regulatory Basis

10 CFR 830.120 Quality assurance requirements Location: (b)(1)
DOE/RL-96-0006 4.1.6.1 Quality Assurance-Quality Assurance Application
DOE/RL-96-0006 4.1.6.2 Quality Assurance-Established Techniques and Procedures

Safety Criterion: 7.3 - 2

A written Quality Assurance Program (QAP) shall be developed, implemented, and maintained. The QAP shall describe the organizational structure, functional responsibilities, levels of authority, and interfaces for those managing, performing, and assessing the work. The QAP shall describe management processes, including planning, scheduling, and resource considerations.

Implementing Codes and Standards

ASME NQA-1-1989
Section 2, "Quality Assurance Program" (including associated supplements)

Regulatory Basis

10 CFR 830.120 Quality assurance requirements Location: (a)(1)
10 CFR 830.120 Quality assurance requirements Location: (c)(1)(i)
DOE/RL-96-0006 4.1.1.6 Defense in Depth-Human Aspects
DOE/RL-96-0006 4.1.4.1 Safety/Quality Culture-Safety/Quality Culture
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (6)

Safety Criterion: 7.3 - 3

Personnel shall be trained and qualified to ensure they are capable of performing their assigned work. Personnel shall be provided continuing training to ensure that job proficiency is maintained.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(1)(ii)*

Safety Criterion: 7.3 - 4

Documents shall be prepared, reviewed, approved, issued, used, and revised to prescribe processes, specify requirements, or establish design. Records shall be specified, prepared, reviewed, approved, and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
Section 3S-1, 7, "Documentation and Records" (including associated supplements)
Section 3S-1, 17, "Quality Assurance Records" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(1)(iv)*

Safety Criterion: 7.3 - 5

Work shall be performed to established technical standards and administrative controls using approved instructions, procedures, or other appropriate means. Items shall be identified and controlled to ensure their proper use. Items shall be maintained to prevent their damage, loss, or deterioration. Equipment used for process monitoring or data collection shall be calibrated and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
Section 3, "Design Control" (including associated supplements)
Section 5, "Instructions, Procedures, and Drawings" (including associated supplements)
Section 8, "Identification and Control of Items" (including associated supplements)
Section 9, "Control of Processes" (including associated supplements)
Section 12, "Control of Measuring and Test Equipment" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(2)(i)*
DOE/RL-96-0006 *4.1.6.3 Quality Assurance-Established Techniques and Procedures*

Safety Criterion: 7.3 - 6

Processes to detect and prevent quality problems shall be established and implemented. Items, services, and processes that do not meet established requirements shall be identified, controlled, and corrected. Correction shall include identifying the causes of problems and preventing recurrence. Item characteristics, process implementation, and other quality-related information shall be reviewed and the data analyzed to identify items, services, and processes needing improvement.

Implementing Codes and Standards

ASME NQA-1-1989
- Section 15, "Control of Nonconforming Items" (including associated supplements)
- Section 16, "Corrective Action" (including associated supplements)

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(1)(iii)*
DOE/RL-96-0006	*4.1.4.1 Safety/Quality Culture-Safety/Quality Culture*	

Safety Criterion: 7.3 - 7

Inspection and testing of specified items, services, and processes shall be conducted using established acceptance and performance criteria. Equipment used for inspections and tests shall be calibrated and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
- Section 10, "Inspections" (including associated supplements)
- Section 11, "Test Control" (including associated supplements)
- Section 12, "Control of Measuring and Test Equipment" (including associated supplements)

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(2)(iv)*

Safety Criterion: 7.3 - 8

Managers shall assess their management processes. Problems that hinder the organization from achieving its objectives shall be identified and corrected.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Chapter: 10.0 Assessments

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(3)(i)*

Safety Criterion: 7.3 - 9

Independent assessment shall be planned and conducted to measure item and service quality, to measure the adequacy of work performance, and to promote improvement. The group performing independent assessments shall have sufficient authority and freedom from the line to carry out its responsibilities. Persons conducting independent assessments shall be technically qualified and knowledgeable in the areas assessed.

Implementing Codes and Standards

ASME NQA-1-1989
Section 18, "Audits" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(3)(ii)*

Safety Criterion: 7.3 - 10

Compliance audits shall be performed at least every three years to verify that the procedures and practices developed to ensure nuclear and process safety are adequate and are being followed. The compliance audit shall be conducted by at least one person knowledgeable in the process. A report of the findings of the audit shall be developed. An appropriate response shall be determined and documented for each of the findings of the compliance audit, and it shall be documented when deficiencies have been corrected. Employers shall retain the two most recent compliance audit reports.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.4 Compliance Audits
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 *5.2.12 Compliance Audits*

Safety Criterion: 7.3 - 11

Procured items and services shall meet established requirements and perform as specified. Prospective suppliers shall be evaluated and selected on the basis of specified criteria. Processes to ensure that approved suppliers continue to provide acceptable items and services shall be established and implemented.

Implementing Codes and Standards

ASME NQA-1-1989
Section 7, "Control of Purchased Items and Services" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(2)(iii)*

Safety Criterion: 7.3 - 12

Changes made to the Quality Assurance Program (QAP) shall be submitted annually to the regulator for review. The submittal shall identify the changes, the pages affected, the reason for the changes, and the basis for concluding that the revised QAP continues to satisfy the requirements of this section.

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (b)(3)*

7.4 Unreviewed Safety Questions

Safety Criterion: 7.4 - 1

A safety evaluation shall be performed to determine whether a situation involves an unreviewed safety question (USQ) for:

(1) Temporary or permanent changes in the facility as described in the existing authorization basis

(2) Temporary or permanent changes in the procedures as derived from existing authorization basis

(3) Tests or experiments not described in the existing authorization basis

A situation involves a USQ if:

1) the probability of occurrence or the radiological or chemical consequences of an accident or malfunction of equipment Important to Safety, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility analysis, may be increased

2) a possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis, may be created

3) any margin of safety is reduced

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*
DOE/RL-96-0006	*5.2.9*	*Management of Change*

Safety Criterion: 7.4 - 2

Regulatory approval shall be obtained for situations determined to involve an unreviewed safety question or a change in a technical safety requirement, prior to initiating the activity, if the initiation of the activity would itself involve a USQ, or implementing the proposed change.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*

Safety Criterion: 7.4 - 3

Procedures shall be developed and implemented to govern the need for, and the performance of, safety evaluations.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Safety Criterion: 7.4 - 4

When information is identified that indicates a potential inadequacy of previous analyses as defined in the approved Safety Analysis Report (SAR) or that indicates a possible reduction in safety margins as defined in the technical safety requirements, the following actions shall occur:

(1) Notify the regulator of the situation upon discovery of the information

(2) Perform a safety evaluation

(3) Take action as appropriate to place or maintain the facility in a safe condition until the safety evaluation is completed

(4) Submit the completed safety evaluation prior to removing any operational restrictions initiated

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations

Safety Criterion: 7.4 - 5

For all safety evaluations required under this section, the following actions shall occur:

(1) Document the basis for the USQ(s) determination.

(2) Incorporate in the existing SAR and technical safety requirements for the facility any changes that are needed as a result of the safety evaluation or any action taken pursuant to this section.

(3) Submit to DOE, on a schedule corresponding to the updates of the SAR for the facility, a report summarizing all situations for which a safety evaluation was required by this section and indicating all “changes” considered in a safety evaluation and implemented 3 months or more before the submittal date of the safety analysis report.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation
Section: 3.16.4 Unreviewed Safety Questions

7.5 Conduct of Operations

Safety Criterion: 7.5 - 1

A program for conduct of operations at the facility shall be established and implemented using a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations

Safety Criterion: 7.5 - 2

The conduct of operations program shall address:

(1) Operations organization and administration
(2) Shift routines and operating practices
(3) Control area activities
(4) Communications
(5) Control of on-shift training
(6) Investigation of abnormal events
(7) Notifications
(8) Control of equipment and system status
(9) Lockout and tagout
(10) Independent verification
(11) Logkeeping
(12) Operations turnover
(13) Operations aspects of facility chemistry and unique processes
(14) Required reading
(15) Timely orders to operators
(16) Operations procedures
(17) Operator aid postings
(18) Equipment and piping labeling
(19) Emergency operating procedures for dealing with responses to accident conditions.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations

Regulatory Basis

DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*
DOE/RL-96-0006	*4.3.1.3*	*Conduct of Operations-Emergency Operating Procedures*
DOE/RL-96-0006	*4.3.1.4*	*Conduct of Operations-Readiness*

7.6 Maintenance

Safety Criterion: 7.6 - 1

A maintenance program for the facility shall be developed and implemented using a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 4.2.1 Engineered Features

Safety Criterion: 7.6 - 2

The maintenance program shall contain provisions sufficient to preserve, predict, and restore the availability, operability, and reliability of structures, systems, and components designated as Important to Safety.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI)

Regulatory Basis

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance

Safety Criterion: 7.6 - 3

The maintenance program for Important to Safety Structures, systems and components shall clearly define:

(1) The Important to Safety structures, systems, and components that comprise the facility

(2) The requirements of the maintenance program that are derived from the program elements listed in Safety Criterion 7.6-4

(3) The management systems used for those activities, including the means for monitoring and measuring the effectiveness of the program and the management of maintenance backlog

(4) The assignment of responsibilities and authority for all levels of the maintenance organization

(5) Mechanisms to feedback such relevant information as trend analysis and instrumentation performance/reliability data in order to identify necessary program modifications

(6) Provisions for identifying and evaluating possible component, system design, occupational safety and health, or other relevant problems and implementation of a self-assessment program

(7) Performance indicators and criteria to be utilized to measure equipment, systems, and personnel effectiveness in maintenance activities

(8) Interfaces between maintenance and other organizations (e.g., involving operations, engineering, quality, and safety)

(9) Quantitative reliability target values for systems and components to start or run, when such values are credited in safety analysis

(10) Appropriate authorization is received before modification starts on a safety instrumented system

(11) Assessment of impact of the modification on the functionality of the safety instrumented system is performed, to ensure functionality is not impaired

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.10 Classification of Structures, Systems, and Components
- Section: 3.2 Safety Responsibilities
- Section: 3.4 Safety/Quality Culture
- Section: 3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI)
- Section: 3.16.3 Incident Investigations
- Section: 3.16.5 Performance Monitoring
- Section: 3.16.6 Performance Indicators
- Section: 3.16.8 Feedback and Trending
- Chapter: 10.0 Assessments

24590-WTP-SRD-ESH-01-001-02, Attachment A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 4.2.7.1 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Reliability

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance-Operational Testing, Inspection, and Maintenance

Safety Criterion: 7.6 - 4

The maintenance program shall address each of the following elements:

(1) Organization and administration
(2) Maintenance training and qualification
(3) Maintenance facilities, equipment, and tools
(4) Types of maintenance
(5) Maintenance procedures and other work-related documents
(6) Planning, scheduling, and coordinating maintenance activities
(7) Control of maintenance activities
(8) Post-maintenance testing
(9) Procurement of parts, materials, and services
(10) Material receipt, inspection, handling, storage, retrieving, and issuance
(11) Control and calibration of measuring and test equipment
(12) Maintenance tools and equipment control
(13) Documented facility condition inspections to identify and address aging effects
(14) Management involvement with facility operations
(15) Maintenance history and trending
(16) Analysis of maintenance-related problems
(17) Modification work.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.11 Quality Levels
Section: 4.2.2 Training and Procedures
Section: 5.3 Configuration Management
Section: 5.4 Compliance Audits
Section: 5.6.5 Mechanical Integrity
Chapter: 11.0 Organization Roles, Responsibilities, and Authorities

Regulatory Basis

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance
DOE/RL-96-0006 5.2.7 Mechanical Integrity
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

7.7 Reporting and Incident Investigation

Safety Criterion: 7.7 - 1

Each incident which resulted in, or could reasonably have resulted in a major accident shall be investigated. An incident investigation shall be initiated as promptly as possible, but not later than 48 hours following the incident.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations
Section: 5.6.7 Investigations of Incidents

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 2

An incident investigation team shall be established and consist of at least one person knowledgeable in the process involved, including a subcontract employee if the incident involved work of the subcontractor, and other persons with appropriate knowledge and experience to thoroughly investigate and analyze the incident. A report shall be prepared at the conclusion of the investigation which includes at a minimum:

(1) Date of incident

(2) Date investigation began

(3) A description of the incident

(4) The factors that contributed to the incident

(5) Any recommendations resulting from the investigation

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations
Section: 5.6.7 Investigations of Incidents
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 3

A system shall be established to promptly address and resolve the incident report findings and recommendations. Resolutions and corrective actions shall be documented. The report shall be submitted to the regulator for evaluation and in support of regulatory oversight. The report shall be reviewed with all affected personnel whose job tasks are relevant to the incident findings including subcontract employees where applicable. Incident investigation reports shall be retained for five years.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.7 Investigations of Incidents

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 4

The Facility Manager shall categorize reportable incidents as soon as reasonably possible and in all cases within 2 hours of identification of the event or condition. If categorization is not clear, the occurrence shall be conservatively categorized at the higher level being considered. The occurrence categorization shall be elevated, maintained, or lowered, as appropriate, as further information is obtained.

Reportable occurrences shall be categorized in accordance with the following guidance:

"Emergencies" are the most serious reportable occurrences and they require an increased alert status for on-site personnel and, in specified cases, for off-site authorities. Emergencies require a time-urgent notification as part of the facility's comprehensive emergency management program.

"Unusual Occurrences" are the category of non-emergency reportable occurrences that exceed the off-normal occurrence threshold and have significant impact or potential for impact on safety, the environment, health, safeguards and security, or operations.

"Off-Normal Occurrences" are the category of abnormal or unplanned reportable occurrences that adversely affect, potentially affect, or are indicative of degradation in the level of safety, safeguards and security, environmental or health protection, performance or operation of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.7 Investigations of Incidents

Safety Criterion: 7.7 - 5

The Facility Manager shall orally notify the regulator of Emergencies within 15 minutes. In addition, the Facility Manager shall orally notify the regulator of Unusual Occurrences, as soon as practical, but in all cases within 2 hours of categorization. The Facility Manager shall contact the regulator via the Headquarters Emergency Operations Center.

Follow-up Notification. The Facility Manager shall provide follow-up oral notification to the regulator via the Headquarters Emergency Operations Center within two hours of identification of further degradation in the level of safety of the facility or other worsening conditions. A change in a reporting level to an Emergency level is to be orally reported within 15 minutes of the recategorization.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations

Safety Criterion: 7.7 - 6

The Facility Manager shall provide written notification of all reportable occurrences, including summaries of Emergencies, to the regulator before the close of the next business day from the time of categorization of the occurrence (not to exceed 80 hours). An Update Occurrence Report shall be submitted when significant new information (including any changes in categorization) is available.

Completion of the Final Occurrence Report is required when the analysis of the occurrence has been completed, root cause and contributing cause(s) finalized, corrective action(s) determined and scheduled, and lessons learned identified. The Final Occurrence Report shall be submitted to the regulator within 45 days of categorization of the occurrence.

The Occurrence Report shall contain, at a minimum, the following information about each reportable occurrence at the facility:

(1) An alphanumeric occurrence report number identifying the regulatory field office, the contractor, the facility, the year of the occurrence, and the sequential number of the occurrence

(2) The number of occurrences in the report

(3) Category of the occurrence

(4) Regulatory program office responsible for the facility involved

(5) All systems, equipment, structural items, administrative controls, or procedures involved in the occurrence or defect identification, including information related to manufacturers, types, model numbers, size, procedure numbers, and (for defect identification) the number of affected components

(6) Date and time when the occurrence was discovered and categorized

(7) Date and time of notification of regulatory and state and local authorities

(8) A thorough and complete description of what occurred or the defect reported, including a sequence of events and a description of failures (or potential failures and the safety significance with respect to defect identification), so that regulatory and contractor personnel, not familiar with the facility-specific design features or administrative controls employed, can understand the complete occurrence and any substantial safety hazard which could result

(9) Operational status of the facility or equipment at the time of the occurrence, including the status of structures, systems, or components that were inoperable at the start of the event and that contributed to the event

(10) Immediate or remedial actions taken to place the facility, system, or equipment in a safe, stable condition, to return them to service, or to correct or alleviate the anomalous condition, and the results of those actions

(11) Cause of the occurrence, including direct and contributing causes and the root cause

(12) Recommendations about whether further evaluation is required and, if so, before or after returning the facility to operation

(13) Action taken or planned to correct the problem and the identified cause and to prevent recurrence

(14) Impact of the occurrence on the environment, health and safety of workers, the public, and on-site and off-site environs (including quantities and types of radioactive materials released)

(15) Levels and types of contamination, human exposures, and known or projected environmental, safety, and health impacts

(16) Impact of the occurrence on the affected program and/or project

(17) Impact of the occurrence on the adequacy of national codes and standards and regulatory requirements

(18) Lessons learned from the occurrence that could be of importance to other facility operators or that shall be addressed in personnel training or facility procedures

(19) Any previous similar events at the same facility that are known to the Facility Manager

(20) The name and telephone number of a person within the Facility Manager's organization who is knowledgeable about the occurrence

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations

Regulatory Basis

DOE/RL-96-0006 *4.3.1.8 Conduct of Operations-Operational Events*

Safety Criterion: 7.7 - 7

Procedures shall be written and implemented to carry out categorization, notification, and reporting requirements for reportable occurrences.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations
Section: 5.6.7 Investigations of Incidents

Safety Criterion: 7.7 - 8

The services of the Environment Safety & Health (ES&H) reporting system, maintained by the Office of Environment, Safety, and Health, shall be used to meet the documentation and distribution requirements of this section.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations

Safety Criterion: 7.7 - 9

The RPP-WTP contractor shall ensure that subcontractors and suppliers report defective items, materials, and services and shall specify these requirements in applicable procurement documents.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.2 Control of Subcontractors

7.8 Emergency Preparedness

Safety Criterion: 7.8 - 1

An emergency response program shall be developed, documented, and implemented for the purpose of protecting public health and the environment. The program shall include the following elements:

(1) An emergency response plan.

(2) Emergency Planning Implementing Procedures to ensure the timely and effective implementation of the provisions of the emergency plan.

(3) A facility emergency response organization, with clearly defined roles, responsibilities and authorities.

(4) A training program that provides initial and annual refresher training for facility response personnel, general employees, and response personnel from other agencies.

(5) Program administration to include maintenance of technical support documents, plans, and procedures, the coordination of activities, and maintenance of appropriate auditable records.

(6) Adequate emergency facilities and equipment to support response.

(7) The scope of the program will be designed to be commensurate with the hazards present at the facility and will be determined by performing an assessment of the hazards.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

Safety Criterion: 7.8 - 2

The Emergency Management Program will be documented in an emergency plan which describes the provisions for responses to Operational Emergencies. The emergency response plan will address the following program elements

(1) The establishment and maintenance of a facility emergency response organization with clearly specified authorities and responsibilities for emergency response and mitigation.

(2) Provisions for interfaces and coordination with Hanford Site and offsite agencies in the areas of planning, preparedness, response, and recovery.

(3) A description of the hazards and potential consequences resulting from analyzed accidents.

(4) Identify and describe the capabilities for the detection of emergency events, the methodology for determining event severity and the basis for declaring an emergency.

(5) The methods to be used to provide notification of an emergency event to Hanford Site organizations, offsite response agencies, and Federal, state and local regulatory agencies.

(6) Provisions for assessing the consequences resulting from the release of hazardous materials.

(7) A description of protective actions for responders, workers, and the public, to include provisions for sheltering, evacuation, and personnel accountability.

(8) Medical support during emergency response, to include provisions for ambulance/hospital services and decontamination of injured personnel.

(9) Methodology for the safe-shut down of the facility, reentry to the facility during or after emergency response and provisions for developing a recovery strategy following an accident.

(10) A public information program designed to provide the public, media and employees with accurate and timely information.

(11) A training program will de designed to ensure that personnel are prepared to respond to, manage, mitigate, and recover from emergencies associated with facility operations.

(12) Provisions for the administration of the program, to include a designated program administrator, program assessment and issue resolution, the development and maintenance of technical support documents, plans, and procedures, the coordination of activities, and maintenance of appropriate auditable records.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006	*4.1.2.3*	*Safety Responsibility-Site and Technical Support*
DOE/RL-96-0006	*5.2.11*	*Emergency Planning and Response*

Safety Criterion: 7.8 - 3

Emergency plans shall be prepared before the startup of the facility, and shall be exercised periodically to ensure that protection measures can be implemented in the event of an accident that results in, or has the potential for, unacceptable releases of radioactive materials within and beyond the facility control perimeter.

A determination shall be made of the size of the geographic area surrounding the facility, known as the Emergency Planning Zone (EPZ), within which special planning and preparedness activities will be performed to reduce the potential health and safety impacts from an event involving hazardous materials. The extent of planning and preparedness necessary shall correspond to the type and scope of hazards present and the potential consequences of events.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.18 Emergency Planning
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.3 Emergency Preparedness-Establishment and Continued Exercise of Emergency Plans*

Safety Criterion: 7.8 - 4

The results of analyses of the facility response to accidents with the potential for releases resulting in doses in excess of Environmental Protection Agency and the State of Washington emergency clean-up standards, beyond the RPP-WTP controlled area boundary shall be used in preparing emergency operating procedures which will contain specific instructions for facility operations personnel on the shutdown of facility processes and the mitigation of accidents for all identified off-normal and emergency conditions.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.2 Emergency Preparedness-Accident Management Strategy*

Safety Criterion: 7.8 - 5

The emergency response plan shall be coordinated with the DOE Hanford Site and local community emergency response plans.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.1 Emergency Preparedness-Offsite Measures*

8.0 Deactivation and Decommissioning

Safety Criterion: 8.0 - 1

There shall be an approved plan for deactivation of the facility before it is constructed. The objectives of the plan shall be to reduce radiation exposure to Hanford Site personnel and the public both during and following deactivation and decommissioning activities and to minimize the quantity of radioactive waste generated during deactivation, decontamination, and decommissioning. Features and procedures that simplify and facilitate decommissioning shall be identified during the planning and design phase based upon a proposed decommissioning method.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix F, Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning

Regulatory Basis

DOE/RL-96-0006 4.2.3.3 Radiation Protection-Deactivation, Decontamination, and Decommissioning Design
DOE/RL-96-0006 4.3.2.3 Radiation Protection-Final Deactivation Plans and Provisions

Safety Criterion: 8.0 - 2

Facilities shall be designed to simplify decontamination and decommissioning, reduce exposure to site personnel and the public during these activities, and increase the potential for reuse. Features and procedures that simplify and facilitate decontamination, decommissioning, and minimization of contaminated equipment and the generation of radioactive waste during deactivation, decontamination, and decommissioning shall be identified during the planning and design phase based upon a proposed decommissioning method or conversion to other use.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix F, Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning
DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 1002
DOE/RL-96-0006 4.2.3.3 Radiation Protection-Deactivation, Decontamination, and Decommissioning Design
DOE/RL-96-0006 4.3.2.3 Radiation Protection-Final Deactivation Plans and Provisions

9.0 Documentation and Submittals

Safety Criterion: 9.0 - 1

An annual report shall be prepared and submitted to the Regulator and appropriate local officials. The annual report shall document:

(1) the quantity of each of the principal radionuclides in excess of background released to unrestricted areas in liquid and gaseous effluents during the previous year of operation.

(2) the calculated annual dose to the maximally exposed members of the public, and (3) the calculated collective dose to members of the public from exposures to RPP-WTP radiation sources.

Reports on dose estimates to the public shall include relevant site-specific information, including the locations of members of the public subject to the greatest potential exposures, the population distribution subject to exposures from RPP-WTP activities, and exposure pathways germane to the site. Values of assumed default or site-specific parameters used in calculations shall be discussed and included with the documentation of the calculations.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 104
40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 94

Safety Criterion: 9.0 - 2

The Contractor should request authorization for construction only after being satisfied by appropriate internal assessments that the main safety issues have been satisfactorily resolved and that the remainder are amenable to solution before operations are scheduled to begin.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

DOE/RL-96-0006 4.4.3 Recommendation for Initiation of Construction

Safety Criterion: 9.0 - 3

The results of the pre-startup safety review should be submitted to DOE for evaluation and in support of authorization decisions and regulatory oversight.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

DOE/RL-96-0006 5.2.6 Pre-startup Safety Review

Safety Criterion: 9.0 - 4

Material that is part of the authorization basis shall be established, documented, and submitted to the DOE for evaluation and in support of decisions and regulatory oversight. The material shall be maintained current with respect to changes made to the facility design and administrative controls and in the light of significantly new safety information.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1 Content of the Authorization Basis
Section: 3.3.2 Control of the Authorization Basis
Section: 3.3.3 Changes to Safety Documentation

9.1 Safety Analysis Reports

Safety Criterion: 9.1 - 1

Safety analyses shall be performed using a tailored approach to develop and evaluate the adequacy of the authorization basis for the facility. Preliminary and Final Safety Analysis Reports shall be prepared to document the safety analyses.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix A, "Implementing Standard for Safety Standards and Requirements Identification"
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Regulatory Basis

DOE/RL-96-0006	*4.1.3.1*	*Authorization Basis-Authorization Basis*
DOE/RL-96-0006	*4.2.1.3*	*Design-Safety Analysis*

Safety Criterion: 9.1 - 2

A SAR shall contain sections that address the following topics:

(1) Site Description
(2) Facility and Process Description
(3) Integrated Safety Analysis
(4) Nuclear Criticality Safety
(5) Technical Safety Requirements
(6) Radiation Safety
(7) Chemical Safety
(8) Fire Safety
(9) Human Factors
(10) Emergency Preparedness
(11) Management Organization
(12) Conduct of Operations
(13) Procedures
(14) Training and Qualification
(15) Deactivation and Decommissioning
(16) Incident Investigations
(17) Records Management
(18) Audits and Assessments
(19) Quality Assurance
(20) Initial Surveillance and In-Service Testing
(21) Maintenance

The SAR should also contain an Executive Summary that provides an overview of the facility safety basis and presents information sufficient to establish a top-level understanding of the facility, its' operation, and the results of the safety analysis.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Safety Criterion: 9.1 - 3

A Preliminary Safety Analysis Report (PSAR) shall be submitted to the regulator only after all major safety issues have been resolved and other safety issues scheduled for completion. The PSAR shall document the facility design and plans for construction and demonstrate adequate planning for the operational phase.

A Final Safety Analysis Report (FSAR) shall be submitted to the regulator for approval prior to authorization to operate a the facility. The FSAR shall document the completed design and construction and provide details on the plans for operation. The FSAR shall include facility and process drawings and fabrication and construction specifications important to the safety analysis of the facility. The FSAR shall identify significant changes made in the facility design and plans for operation from what was presented in the PSAR.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Safety Criterion: 9.1 - 4

The FSAR shall be reviewed annually and updated as necessary to ensure that the information is current, remains applicable, and reflects all changes implemented up to 3 months prior to the filing of the updated FSAR. The regulatory approval of any Unreviewed Safety Questions, and the material submitted to the regulator in support of that approval, shall be considered an addendum to the FSAR until the information is incorporated into the FSAR as part of the next periodic update.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.1 - 5

The SAR shall be maintained as a controlled document.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.1 - 6

All responsibilities concerning the facility as identified in the approved SAR shall be carried out.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.2 Safety Responsibilities

Safety Criterion: 9.1 - 7

The hazard analysis shall be submitted for approval as part of the SAR.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 9.0 Scheduling of Safety-Related Activities

Regulatory Basis

9.2 Technical Safety Requirements

Safety Criterion: 9.2 - 1

Technical safety requirements shall be prepared and submitted for approval, and the facility shall be operated in accordance with the approved technical safety requirements.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations
Section: 3.3.1.4 Technical Safety Requirements (TSR)

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.2 - 2

Technical safety requirements shall be based on the Final Safety Analysis Report and any facility-specific commitments made.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements

Safety Criterion: 9.2 - 3

Technical safety requirements shall consist of the following:

(1) Safety Limits (SLs). This section of the technical safety requirements shall contain the safety limits on the process variables. If an SL for a nuclear facility is exceeded, the nuclear facility shall be immediately placed in the most stable, safe condition attainable, including total shutdown, except where such action might reduce the margin of safety. The safe, stable condition entered as a corrective action shall be maintained until DOE authorizes further operations.

(2) Operating Limits:

(a) Limiting Control Settings (LCSs). This section of the technical safety requirements shall contain the settings for automatic alarms and for the automatic or non-automatic initiation of protective actions related to those variables associated with the function of Safety Design Class structures, systems, or components (SSCs) (if the safety analyses show that they are relied upon to mitigate or prevent an accident). The specific settings chosen must correct a situation automatically or manually such that the related SL is not exceeded. If an automatic alarm or protective device does not function as required during an applicable operating mode, the contractor shall take action as defined in the LCS to maintain the variables within the requirements and to repair the automatic device promptly or to shut down the affected part of the process and, if required, to shut down the facility.

(b) Limiting Conditions for Operation (LCOs). This section of the technical safety requirements shall contain the limits on functional capability or performance level. If a limiting condition for operation is not met, the contractor shall take any remedial actions specified by the technical safety requirements until the condition can be met.

The LCOs will be based upon:

(a) Process variables, design features, and operating restrictions that are the initial conditions for accident analysis.

(b) Structures, systems, and components that must function to prevent or mitigate accidents to achieve compliance to offsite radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2.

(3) Surveillance Requirements (SRs). This section of the technical safety requirements shall contain the surveillance requirements necessary to maintain operation of the facility within the SLs, LCSs, and LCOs. If a required surveillance is not successfully completed or is not performed with its required frequency, the systems or components involved shall be assumed to be inoperable and actions defined by LCSs or LCOs shall be taken until the systems or components can be shown to be operable.

(4) Administrative Controls. This section of the technical safety requirements shall contain the requirements associated with administrative controls, including those for reporting violations of the technical safety requirements. Staffing requirements for facility positions important to safe operation of the facility shall be included in the administrative controls section of the technical safety requirements. Commitments to the safety management programs identified in the SAR as necessary components of the facility safety basis shall be provided in this section.

(5) Use and Application. This section of the technical safety requirements shall contain the basic instructions for applying the safety restrictions contained in the technical safety requirements. Definitions of terms, operating modes, frequency notations, and actions to be taken in the event of violations of OLs or SRs are to be included in this section.

(6) Appendices.

(a) Basis. This appendix shall provide summary statements of the reasons for the OLs and associated SRs. The basis shall show how the numeric value, the condition, or the surveillance fulfills the purpose derived from the safety documentation. The primary purpose for describing the basis of each requirement is to ensure that any future changes to the requirement will not affect its original intent or purpose.

(b) Design Features. This appendix shall describe design features of the facility that, if altered or modified, would have a significant effect on safe operation. If design features are described in a regulator-approved SAR pursuant to this part, this appendix is not required.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)

Regulatory Basis

DOE/RL-96-0006 4.3.1.6 Conduct of Operations-Operations Within the Authorization Basis

Safety Criterion: 9.2 - 4

Technical safety requirements shall be kept current at all times so that they reflect the facility as it exists and as it is analyzed in the SAR.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.2 - 5

All proposed revisions to technical safety requirements, excluding its bases, shall be submitted for regulatory approval prior to implementation of the revision. The submission shall include the basis for the proposed revision.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation

Safety Criterion: 9.2 - 6

Only current approved technical safety requirements shall be used for the operation of the facility. Technical safety requirements shall be maintained as a controlled document with all users designated as authorized users.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements
Chapter: 8.0 Document Control and Maintenance

9.3 Risk Management Plan (this section has been deleted)

Safety Criterion: 9.3 - 1

This safety criterion has been deleted.

All text on this page has been deleted.

Safety Criterion: 9.3 - 2

This safety criterion has been deleted.

Safety Criterion: 9.3 - 3

This safety criterion has been deleted.

Safety Criterion: 9.3 - 4

This safety criterion has been deleted.

Safety Criterion: 9.3 - 5

This safety criterion has been deleted.

Appendix A

Implementing Standard for Safety Standards and Requirements Identification

CONTENTS

1.0 Introduction A-1
2.0 Process Initiation A-1
3.0 Identification of Work A-2
4.0 Hazard Evaluation A-3
4.1 Identification of Hazards A-4
4.2 Identification of Potential Accident/Event Sequences A-4
4.3 Estimation of Consequences A-4
4.3.1 Accident Severity Level Identification A-4
4.3.2 Accident Analysis A-5
4.3.3 Normal Conditions A-6
4.4 Estimation of Accident Frequencies A-7
4.5 Consideration of Common Cause/Common Mode failures A-7
4.6 Definition of Design Basis Events A-8
4.7 Definition of Operating Environment A-8
4.8 Identification of Potential Controls A-8
4.9 Documentation A-9
5.0 Development of Control Strategies A-10
6.0 Classification of Structures, Systems, and Components A-14
7.0 Identification of Standards A-16
8.0 Confirmation of Standards A-18
9.0 Formal Documentation A-18
10.0 Recommendation A-18
11.0 Definitions A-19

1.0 Introduction

This standard implements the process for establishing a set of radiological, nuclear, and process safety requirements and standards as described in DOE/RL-96-0004 and RL/REG-98-17. The Project refers to this process as Integrated Safety Management (ISM).

The activities described below establish radiological, nuclear and process safety standards and requirements for design, construction, and operation of the facility. Establishment of safety standards and requirements is an iterative process that takes place throughout the life of the project. As the design evolves, the process repeatedly evaluates these standards and requirements based on the evolving design.

The Safety Requirements Document (SRD) provides formal documentation of the standards, which are a result of this process. The SRD is updated as required to reflect the results of successive iterations of the standards and requirements identification process (i.e., the ISM process).

2.0 Process Initiation

The RPP-WTP Project Manager shall ensure implementation of the Project Management Plan, thus assuring that adequate resources with appropriate technical background are available and organized to perform subsequent tasks. This activity also assures that the input information required for the safety standards and requirements identification process has been collected and organized. This input information includes the top-level safety standards and principles stipulated by DOE in DOE/RL-96-0006 and the laws and regulations applicable to the RPP-WTP project.

The DOE/RL-96-0004 safety requirements and standards identification Process Manager for the project is the Radiological, Nuclear, and Process Safety Manager.

The Process Manager chairs the DOE/RL-96-0004 safety requirements and standards identification Process Management Team (PMT). The PMT is constituted in accordance with project implementing documents and includes managers from the following project organizations:

- Environmental, Safety, & Health
- Engineering
- Operations

The Process Management Team shall oversee the ISM process and shall provide resources and resolve issues as necessary. The PMT shall set up integrated teams for the conduct of ISM on a plant system basis. Individual PMT members shall provide various subject matter experts to help fulfill the roles required of the Integrated Teams for conduct of the ISM process.

3.0 Identification of Work

The aim of this activity is to describe the work that will be performed so that the hazards inherent in the work can be identified and evaluated. Work activity experts who have extensive knowledge of the overall processing approach and are integrally associated with the facility design shall perform this activity. work activity experts shall be drawn from the following RPP-WTP organizations:

- Engineering staff
- Operations staff

When appropriate, the PMT may also draw work activity experts from the staff of other departments, such as from Construction.

In an overall sense, identification of work involves definition of the project mission and identification of the processes that must be performed to accomplish the mission. It includes selection of optimum functions, processes, and parameters through trade studies and definition of functional requirements. Identification of work for the purpose of design development involves definition of various plant systems, structures, and components. This latter definition is the focus for the Integrated Teams created to conduct ISM on a plant system basis.

The product of this activity includes:

- Process description
- System descriptions
- Descriptions of key structures
- Basis of design documents
- PFDs, MFDs, and P&IDs

The results of the identification of work activity shall be documented in the SRD by inclusion or by reference.

The identification of work activity is an iterative process. Identification of work will be reconsidered in light of design evolution, the outcome of hazard evaluations, and the development of hazard control strategies.

4.0 Hazard Evaluation

The aim of the hazard evaluation activity is to identify and characterize the hazards resulting from the work. The integrated teams shall conduct the hazard evaluation activity on a plant system basis. These teams shall include work activity experts (as defined in Section 3.0), hazard assessment experts, and hazard control experts.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Safety Analysis Manager and of the Regulatory Safety Manager. The process management team shall provide additional technical resources as required to evaluate the hazards.

The hazard evaluation shall address hazards inherent in normal operation as well as potential accidents resulting from abnormal internal and external events.

The hazard evaluation shall comprise the following elements:

- Identification of Hazards
- Identification of Potential Accident/Event Sequences
- Estimation of Accident Consequences
- Estimation of Accident Frequencies
- Consideration of Common Cause and Common Mode Failures
- Definition of Design Basis Events
- Definition of Operating Environment
- Identification of Potential Control Strategies
- Documentation

These elements are discussed below.

4.1 Identification of Hazards

The objective of this element is to systematically identify the hazards associated with the defined work.

The integrated teams shall compile a list of hazardous materials and energy sources associated with the facility processes, design, and operations. This list shall be compiled based on the identified work. This compilation provides information used to identify potential accidents resulting in the uncontrolled release of hazardous material or energy to workers, the public, and the environment. The team may use checklists to guide the compilation process and to assure that all potential hazards from both natural and manmade sources originating from outside and inside the facility are addressed.

4.2 Identification of Potential Accident/Event Sequences

The objective of this element is to perform a structured and systematic examination of the facility and its operations to identify potential accidents (including common mode and common cause failures). The team shall conduct this examination using methodologies and guidelines in AIChE (1992).

4.3 Estimation of Consequences

4.3.1 Accident Severity Level Identification

A severity level, SL, shall be assigned to each postulated radiological accident. The severity level shall reflect the unmitigated consequences of the postulated accident. Unmitigated consequences shall account for the quantity, form and location of the radioactive material available for release, and the energy sources available to interact with the hazardous material. Unmitigated consequences shall not account SSCs that serve to prevent or mitigate the release. Specifically, unmitigated consequences shall be evaluated on the basis of a ground level release. The severity level shall be defined as follows:

SL	Facility Worker Consequence	Collocated Worker Consequence	Public Consequence
SL-1	> 25 rem/event	> 25 rem/event	> 5 rem/event
SL-2	5 - 25 rem/event	5 - 25 rem/event	1 - 5 rem/event
SL-3	1 - 5 rem/event	1 - 5 rem/event	0.1 - 1 rem/event
SL-4	< 1 rem/event	< 1 rem/event	< 0.1 rem/event

These severity levels are related to the radiological and process standards of SRD Chapter 2.0 as follows:

- The unmitigated consequences associated with SL-1 events exceed the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-2 events are below the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-3 events are below the radiological standards for unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-4 events are below the radiological standards for anticipated events (SRD Safety Criterion 2.0-1).

Consequences to the facility worker shall be evaluated at the worst-case occupied location. Consequences to the collocated worker and the public shall be evaluated at the locations specified in Appendix D to the *Safety Requirements Document, Volume II*.

Early in the design, the severity level is estimated based on the experience of the Integrated Teams. As the design progresses, these estimates are confirmed through the formal accident analyses described in Section 4.3.2. These accident analyses do not address all of the potential accidents identified, but they do address bounding examples of each type of accident. The team should use the results of the accident analyses to validate the severity level estimates for potential accidents not addressed in the formal accident analyses.

The potential consequences of releases of hazardous chemicals shall also be assessed. The assessment shall consider both the inherent hazard of the chemical itself, and the potential for the chemical hazard to initiate or exacerbate a radiological hazard.

4.3.2 Accident Analysis

Accident analyses provide confirmation that the design satisfies the radiological and process standards in the SRD. Accident analyses also provide confirmation of the severity levels assigned to potential accidents.

The formal accident analyses shall address design basis external events and natural phenomena as well as postulated internal events.

The postulated internal events shall be grouped by type. Accident types applicable to the RPP-WTP include the following:

- Liquid spills
- Spills of solid materials
- Pressurized releases
- Chemical reactions
- Boiling
- Flammable gas ignition (e.g., hydrogen in air)
- Fires
- Load drops
- Radiation exposure
- Criticality

As a minimum, the accident analysis shall address the most severe credible event of each type.

Initially, the accident analysis shall evaluate the unmitigated consequences of the postulated accidents. As control strategies are developed, the accident analysis shall also evaluate the impact of the SSCs that implement the control strategy on the potential consequences.

The accident analysis shall consider the following factors:

- Inventory of material at risk in the scenario.
- The respirable release fraction for the accident scenario. This is a function of the composition of the material at risk, of the form of the material, and of the interaction between the material at risk and the energy available in the accident scenario.
- The fraction of the airborne material released to potentially occupied locations or the environment.
- Bounding atmospheric dispersion coefficients (if appropriate).
- Radiological composition of the material released.
- External radiation field.
- Exposure times.

The accident analysis shall address the potential consequence to facility workers, collocated workers, and the public.

4.3.3 Normal Conditions

Some hazards inherent in normal operation must be mitigated to comply with the standards for normal operation in SRD Chapter 2.0. Such hazards shall be addressed in accordance with the RPP-WTP Radiation Protection Plan.

4.4 Estimation of Accident Frequencies

There is normally insufficient information early in the design to accurately quantify the frequency of postulated internal events because this frequency depends on the design of the SSCs that implement the control strategy used to manage the hazard. At an early stage, frequency evaluations may be based on the team's experience with similar hazards in similar facilities. The team shall validate these estimates as the design develops.

As the design matures, information on the frequency of hazardous events is gained from the use of hazard evaluation techniques that provide frequency data (i.e., HAZOP, FMEA, Event Trees, and Fault Trees). Evaluations of the frequency of failure in redundant systems or in diverse systems using similar equipment shall consider dependent failures.

The frequencies of design basis external events may be derived from existing analyses (e.g., safety analyses for adjacent facilities), from evaluation of historical data (e.g., transportation data), or from site-specific information (e.g., seismic history).

4.5 Consideration of Common Cause/Common Mode failures

The following are typical common cause events:

- Natural phenomena events
- External man made events
- Loss of electrical power
- Fire
- Internal missiles
- Internal flooding

Common cause events should be treated as discrete events in the hazard analysis. The analyses of common cause events shall focus on identifying provisions to prevent the loss of safety function. The analyses of natural phenomena events shall consider induced effects, such as fire and loss of electrical power.

Common mode failures shall be addressed through dependent failure modeling as required by Section 4.4 above.

4.6 Definition of Design Basis Events

The hazard evaluation shall identify a set of internal design basis events. These events shall be selected to define a set of bounding performance requirements for the SSCs relied upon to control the hazards.

The hazard evaluation shall define a set of external man made design basis events. These events shall be selected based on the results of the hazard analysis to define a set of bounding performance requirements for the SSCs relied upon to mitigate these events.

The integrated teams perform the identification of internal and external design basis events.

Design basis natural phenomena shall be as defined in the SRD Safety Criteria 4.1-3 and 4.1-4.

4.7 Definition of Operating Environment

The hazard evaluation shall define a set of bounding operating conditions in which SSCs relied upon to control hazards must function. Environmental parameters to be addressed include the following:

- Temperature
- Pressure
- Humidity
- Radiation Levels
- Chemical Environment

4.8 Identification of Potential Controls

Based on the experience and judgement of team members, the integrated team shall identify an initial set of potential hazard controls to manage each potential accident. This set of potential hazard controls shall address means of preventing the potential accident and should address means of mitigating the consequences of the accident. The function(s) of each potential hazard control should be clearly described. Potential hazard controls shall be identified to manage accident conditions arising from upsets in the process, conditions arising from external events, and conditions inherent in the normal operation of the process.

4.9 Documentation

The hazard evaluation shall be documented in a hazard analysis report (HAR). The results of the hazard evaluation shall be contained in a hazard database. For each hazard considered, the hazard database shall record the following information produced by the hazard evaluation:

- Hazard identifier
- Hazard description
- Initiators
- Hazard severity level estimate (based on unmitigated consequences)
- Severity level basis
- Assumptions affecting the release (material at risk, energy available, etc)
- Hazard frequency estimate
- Basis for frequency estimate
- Potential controls and functions
- References for the hazard (these would typically be products of the work identification process)

Hazard evaluation documentation shall be included in the SRD by inclusion or by reference. This documentation shall include the following:

- Description of the comprehensive approach to hazard evaluation
- Description of the methodology for identification and quantification of work hazards
- Description of the methodology for identifying potential accident scenarios
- Description of the methodology for consequence assessment
- Clear identification of assumptions (e.g., quantity and form of material at risk, rate of release and relevant process conditions) that may drive or inhibit the potential accident must be clearly identified
- Description of results
- Evidence of appropriate staffing, and adequate technical staffing and structure applied to the hazard evaluation

5.0 Development of Control Strategies

The aim of the development of control strategies activity is to identify a means of controlling each of the hazards identified in the hazard evaluation. The integrated teams of work activity experts, hazard assessment experts, and hazard control experts, as discussed in Sections 3.0 and 4.0, perform this activity.

The PMT members shall provide additional technical resources as required to develop the control strategies.

The integrated teams select preferred control strategies based on the set of potential controls identified by the hazard evaluation team. Selection of the preferred strategy considers the following factors:

- The functions required of the strategy in order to control the hazard
- The degree of defense in depth and reliability provided by the control strategy. The Implementing Standard for Defense in Depth provides guidance in this area.
- Applicable design basis events.
- The operating environment in which the SSCs implementing the control strategy must function.
- Effectiveness and efficiency of the control strategy.
- Conformance with the DOE stipulated top level standards.
- Compliance with applicable laws and regulations.

The control strategy will typically comprise a series of elements including some or all of the following:

- Passive and/or active SSCs that function to prevent the release (that is, SSCs that reduce the probability that a release will occur)
- Passive and/or active SSCs that function to mitigate the release (that is, SSCs that reduce the consequences once a release has occurred)
- Administrative controls (for example, limits on inventory)

Consistent with the defense in depth principle, the control strategy development should emphasize preventive measures. It should also emphasize passive SSCs over active SSCs and retention of released material over dispersion. Ideally, the preferred control strategy should incorporate SSCs that prevent releases and SSCs that mitigate the consequences of a release, should it occur.

Once the preferred control strategy is identified, it shall be evaluated using the techniques described in Section 4.3 through 4.5. In addition, the evaluation of the control strategy shall identify the measures necessary to assure that it performs its functions reliably. Such measures include maintenance requirements, testing intervals and calibration frequency. The results of this evaluation serve to confirm that the control strategy is capable of satisfying SRD Safety Criteria 2.0-1.

If credit is taken for operator action to satisfy the public radiological exposure standards of Safety Criterion 2.0-1, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem TEDE whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy public chemical exposure to the standards of Safety Criterion 2.0-2, provisions for operational access and control are made so that the operator exposure does not exceed the limits specified in Safety Criterion 4.3-7.

Documentation of the hazard control strategy development process shall clearly indicate selection of the control strategies and show the linkage of the control strategies to the respective hazards. The control strategy should be described in terms of the safety functions required (e.g., limit release of radionuclides, etc.) and in terms of a set of engineered features, administrative controls (procedures and training), and management systems selected for implementing the strategy. When the nature of the hazard is such that the appropriate control strategy is self-evident, the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria, and need not provide a discussion of other, nonapplicable control strategies. Similarly, where a proven control strategy that is appropriate to the hazard exists and it is obvious to the team that there are no other alternative control strategies that could be equally attractive, then the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria. Otherwise, the documentation should identify all control strategies considered and provide a defensible rationale for selection of the preferred strategy.

The following information produced by the control strategy definition shall be recorded in the hazard database:

- Preferred control strategy
- Linkage of the control strategy to the respective hazards
- Rationale for preferred control strategy selection
- Defense in depth provided
- Control strategy functions and performance requirements
- Estimate of the unmitigated event frequency
- Estimate of the consequences from the mitigated event
- Estimate of the mitigated event frequency
- Applicable design basis events (e.g., design basis earthquake)

One of the issues in developing a control strategy for a particular hazard is determining the number of layers of prevention and mitigation appropriate for the hazard. The control strategies shall conform to the requirements defined in the Implementing Standard for Defense in Depth. In addition, the following guidance shall be considered in developing control strategies.

The general RPP-WTP design approach is to provide two confinement barriers against the release of hazardous materials. The process vessels and piping form the primary confinement barrier; the process cells and associated ventilation system form the secondary confinement barrier. Releases from the primary confinement are mitigated by the secondary confinement.

The accident severity levels defined in Section 4.3.1 are related to the exposure standards in SRD Safety Criterion 2.0-1. The SRD Safety Criterion 2.0-1 exposure standards are frequency based, so it is possible to establish target frequencies for events with a given severity level. The target frequencies tabulated below are consistent with SRD Safety Criterion 2.0-1.

SL	Event Target Frequency (yr^{-1})
SL-1	$<10^{-6}$
SL-2	$<10^{-4}$
SL-3	$<10^{-2}$
SL-4	$<10^{-1}$

These target frequencies may be used to guide control strategy development as described below.
For SL-1 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.
- Meeting the target frequency will usually require diverse SSCs that act to prevent the release.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the preventive SSCs assure that the frequency of release is less than 10^{-4} per year, but more than 10^{-6} per year. This frequency is not acceptable for events that have SL-1 level consequences, but is acceptable for events that have SL-2 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-2 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-1 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.
- SSCs in control strategies for SL-1 events shall satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-2 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the only viable preventive SSCs assure that the frequency of release is less than 10^{-2} per year, but more than 10^{-4} per year. This frequency is not acceptable for events that have SL-2 level consequences, but is acceptable for events that have SL-3 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-3 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-2 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.
- SSCs in control strategies for SL-2 events should satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-3 and SL-4 events:

- The mitigation provided by the secondary confinement would be adequate to satisfy SRD Safety Criterion 2.0-1. It would also be adequate to satisfy SRD Safety Criteria 1.0-3 through 1.0-5. However, preventive features should be considered consistent with the defense in depth principle.
- A single preventive SSC may satisfy the frequency goal for SL-3 and SL-4 events.
- SSCs in control strategies for SL-3 and SL-4 events need not satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

Notwithstanding the foregoing guidance on control strategy selection, administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control.

6.0 Classification of Structures, Systems, and Components

The design classification process used on the RPP-WTP Project provides a consistent, project-wide approach for the classification of the RPP-WTP SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs can be revised as necessary.

The RPP-WTP project has established a design classification system to provide assurance to DOE that the defined safety functions of SSCs will perform as intended.

SSCs defined as Important-to-Safety for the RPP-WTP include the following:

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs are designated as Safety Design Class, as defined by SRD Safety Criterion 1.0-8.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs are designated as Safety Design Significant, as defined by SRD Safety Criterion 1.0-8.

   The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

   Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded or prevent a criticality. However, additional items may also be designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis.

   Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

When an SSC is designated as Safety Design Class it has the following attributes:

1) Quality Level 1 (QL-1) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
2) For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. If the hazard analysis shows that these requirements are necessary, this requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.
3) The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-3.
4) General design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Class SSCs.
5) Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0.
6) Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.
7) Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements.

When an SSC is classified as Safety Design Significant it is has the following attributes.

1) Quality Level 2 (QL-2) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-4.
3) General and specific design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Significant SSCs.
4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

7.0 Identification of Standards

Identification of standards is an iterative activity. Initially, the set of standards and requirements is derived from a general understanding of the hazards inherent in the work. As the design evolves, the hazard evaluation and the development of the control strategies justify tailoring the set of standards to better fit the hazards.

The identification of engineering/design, manufacture/fabrication, and construction standards is performed by an integrated team including work activity experts, hazard assessment experts, hazard control experts, as discussed in Sections 3.0 and 4.0, and standards experts. Identification of other standards (e.g., quality assurance, conduct of operations, etc.) will be performed by specially constituted teams formed by the PMT. The aim of this activity is to identify a tailored set of standards and requirements that will assure adequate safety when implemented.

The process management team shall provide additional technical resources as required to identify the standards.

Standards experts shall be drawn from the following RPP-WTP organizations:

- Staff of the Engineering Manager
- Technical staff of the ES&H Manager

The standards identified are evaluated and tailored for each control strategy based on compliance with applicable laws and regulations and conformance with the DOE-stipulated top level standards, plus the output of the preceding hazard evaluation and control strategy development steps. Typical considerations include the following:

- The severity level of the hazard
- The number of independent SSCs that comprise the control strategy
- The control strategy functions - recognizing that a specific control strategy may have multiple functions and serve to control multiple hazards
- The service environment
- The applicable design basis events
- The target reliability for the control strategy

The target frequencies described in Section 4 provide a basis for establishing target reliabilities for the SSCs that comprise the control strategy. The combined reliability of the preventive SSCs and the SSCs that provide mitigation must be consistent with the target frequency for the unmitigated event. The reliability of the preventive SSCs should be consistent with the release frequency used to determine the degree of mitigation provided.

Documentation of the standards and requirements identification process provides justification of the set selected and links each control strategy to its associated set of standards. The information generated during standards selection is retained in database form for each control strategy:

- Control strategy
- Service environment
- Applicable design basis events
- Applicable standards
- Performance requirements
- Testing/calibration requirements
- In-service inspection requirements
- Maintenance requirements
- Quality level
- Standards justification

This information is structured so it can be linked to the control strategies in the hazard schedule. This provides a link from the hazards through the control strategies to the standards. Not all of this information will be available early in the design. For example, it will not be possible to define maintenance and testing requirements until the design is mature.

The standards identified through this activity shall be reflected in the SRD.

As the standards are tailored, discrepancies with the current version of the SRD may arise. Such discrepancies shall be recorded. Formal changes to the SRD require approval from DOE.

8.0 Confirmation of Standards

Based on the recommendation of the PMT, the RPP-WTP Project Safety Committee (PSC) Chair requests the PSC to confirm the selected set of standards. The PSC defines a review approach, carries out the review, and documents the findings of the review. Comments by the PSC shall receive formal disposition by the Process Management Team.

9.0 Formal Documentation

Following confirmation by the PSC, the results of the standards selection process shall be documented in the Safety Requirements Document (SRD). The SRD shall incorporate documentation supporting these results by reference. The SRD shall identify and justify the set of requirements and standards selected to provide adequate protection of workers, the public, and the environment.

10.0 Recommendation

The recommended set of standards shall be certified in accordance with project implementing documents. When properly implemented, the set of standards:

1) Provides adequate safety
2) Complies with applicable laws and regulations
3) Conforms with the Top-Level Safety Standards and Principles

11.0 Definitions

Credible event: Any event with a frequency greater than 10^{-6} per year, including allowance for uncertainties.

Important to Safety: Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related, or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related, may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Mitigated event: As used in this standard, a mitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Mitigation of the consequences of the release as provided by the control strategy

Mitigated event frequency: The mitigated event frequency is the corresponding release frequency times the probability that the elements of the control strategy that mitigate the release will function given the release.

Release frequency: The release frequency is the product of the frequency of the initiating event times the probability that all elements of the control strategy that would prevent the release fail, given the initiating event.

Reliability: The probability that an SSC will perform its safety function when required.

Unmitigated event: As used in this standard, an unmitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Failure of all elements of the control strategy that would mitigate the consequences of the release

Unmitigated event frequency: The frequency of an unmitigated event is the corresponding release frequency times the probability that all elements of the control strategy that would mitigate the release fail, given the release.

Appendix B

Implementing Standard for Defense in Depth

CONTENTS

1.0 Introduction B-1
2.0 Standards for the Implementation of Defense in Depth Sub-Principles B-1
2.1 Defense in Depth B-2
2.1.1 Implementing Standards B-2
2.1.2 Discussion B-2
2.2 Prevention B-4
2.2.1 Implementing Standards B-4
2.2.2 Discussion B-4
2.3 Control B-5
2.3.1 Implementing Standards B-5
2.3.2 Discussion B-6
2.4 Mitigation B-7
2.4.1 Implementing Standards B-7
2.4.2 Discussion B-7
2.5 Automatic Systems B-8
2.5.1 Implementing Standards B-8
2.5.2 Discussion B-8
2.6 Human Aspects B-9
2.6.1 Implementing Standards B-9
2.6.2 Discussion B-9
3.0 Determination of SSCs for the Implementation of Defense in Depth B-12
4.0 Definitions B-15
5.0 References B-20
6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth B-21
6.1 DOE O 420.1, Facility Safety (Ref. 5.2) B-21
6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3) B-21
6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7) B-22
6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8) B-22
6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9) B-23
6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11) B-24
6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12) B-25
6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13) B-25

1.0 Introduction

The purpose of this Implementing Standard is to consolidate the standards to be applied in the design, construction, and operation of the RPP-WTP with respect to defense in depth. This Implementing Standard also provides for tailoring of defense in depth as is appropriate to the nature and severity of the hazard and hazardous situations to which it is applied.

Section 2.0 identifies the subordinate standards used in the application of the six defense in depth sub-principles of DOE/RL-96-0006. These subordinate standards are derived, in part, from various available consensus standards. In cases where no relevant consensus standard exists for a given defense in depth sub-principle, this document provides the criteria to be implemented.

Section 3.0 discusses the approach to be used in implementing defense in depth with respect to determining an adequate combination of passive barriers and active SSCs that afford protection against a postulated initiating event.

Terms used in this Implementing Standard are defined in Section 4.0. These definitions are derived from consensus standards, tailored to the work and hazards of the RPP-WTP.

2.0 Standards for the Implementation of Defense in Depth Sub-Principles

The Top Level Principles identify the following sub-principles that must be addressed in order to demonstrate compliance with the principle of defense in depth:

- Defense in depth
- Prevention
- Control
- Mitigation
- Automatic Systems
- Human Aspects

The following subsections contain the standards on application of the six sub-principles of defense in depth from DOE/RL-96-0006 (Ref. 5.4). These consensus standards will be tailored to remove obviously reactor-specific and other non-applicable criteria. In accordance with the DOE/RL-96-0004 process, further tailoring will be performed as the design develops.

The following subsections contain excerpts and extracts from several consensus standards. Where necessary to avoid the implication of misquoting, differences in wording from the cited consensus standards are identified by presenting added words in italics and by inserting double-brackets where words have been removed. Citation of a portion of a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

2.1 Defense in Depth

"To compensate for potential human and mechanical failures, a defense-in-depth strategy should be applied to the facility commensurate with the hazards such that assured safety is vested in multiple, independent safety provisions, not one of which is to be relied upon excessively to protect the public, the workers or the environment. This strategy should be applied to the design and operation of the facility." (DOE/RL-96-0006, Section 4.1.1.1)

2.1.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)
4. IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

2.1.2 Discussion

The RPP-WTP will be designed with the objective of providing multiple *levels* of protection to prevent or mitigate the unintended release of radioactive materials to the environment. Defense in depth will include: siting; minimization of material at risk; the use of conservative design margins and quality assurance; the use of successive physical barriers for protection against the release of radioactivity; the provision of multiple means to control critical safety functions (those basic safety functions needed to control the processes, maintain them in a safe state, and to confine and mitigate radioactivity associated with the potential for accidents with significant [ ] radiological impact *to the public, facility workers or collocated workers*); the use of equipment and administrative controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition; means to monitor accident releases required for emergency responses; and the provision of emergency *preparedness* for minimizing the effects of an accident (Ref. 5.2).

The defense-in-depth concept is integrated into the RPP-WTP design process. The application of the defense-in-depth concept to the facility design helps identify potential safety features to be included in the facility design. Consideration will be given to prevent or mitigate accident consequences from contaminating the environment, even when direct public or worker safety is not an issue.

Defense in depth is a safety design concept or strategy that is applied at the beginning and will be maintained throughout the facility design process. This safety design strategy is based on the premise that no one *level* of protection is completely relied upon to ensure safe operation. This safety strategy provides multiple *levels* of protection to prevent or mitigate an unintended release of radioactive material to the environment.

Conceptually, there are three levels of defense in depth.

1. The first level of defense consists of a well-designed facility with process design to reduce source terms, reliable SSCs that are simple to operate and maintain and resistant to degradation, and personnel well trained in operations and maintenance and committed to a strong safety culture.
2. The second level recognizes that failures of systems and components and human failures cannot be entirely eliminated and that protective features (e.g., engineering design features and administrative controls) are required. These features are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of anticipated, but abnormal events. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.
3. The final level of defense consists of conservatively designed *important to* safety SSCs to prevent or mitigate the consequences of accidents that may be caused by errors, malfunctions, or events that occur both internal and external to the facility (Ref. 5.3).

Implementing Standards for the following elements of defense in depth described in the nonreactor safety Implementation Guide (IG) related to safety design and construction are addressed in the sections of this document that are referenced below.

IG Element	Discussed in Section
Siting	2.2.2
Material at risk	2.2.2
Conservative design	2.2.2
Quality assurance	2.6.2
Physical barriers	2.4.2
Critical safety functions	2.3.2
Equipment and administrative controls	2.3.2 and 2.6.1
Emergency features	2.5.2

When active SSCs are required to achieve defense in depth, RPP-WTP will apply the single failure criterion in accordance with ANSI/ANS-58.9 (Ref. 5.8) for fluid systems and IEEE Std 379 (Ref. 5.9) for electrical and instrumentation and control systems, as discussed below.

The application of the single failure criterion begins with the identification of an initiating event. Initiating events are identified in the normal course of applying integrated safety management in accordance with DOE/RL-96-0004, as described in the RPP-WTP Implementing Standard for Safety Standards and Requirements Identification (i.e., SRD Vol. II, Appendix A). In evaluating the defense in depth of the RPP-WTP, single failures must be postulated in addition to the initiating event (that is the initiating event is not the single failure) (Ref. 5.8). For fluid systems, during the short term, the single failure considered may be limited to an active failure. During the long term, assuming no prior failure during the short term, the limiting single failure considered can be either active or passive. Examples of passive failures are valve packing and pump seal leakage.

Tailoring of the application of the single failure criterion to the work and associated hazards is discussed in Section 3.0.

2.2 Prevention

"Principal emphasis should be placed on the primary means of achieving safety, which is the prevention of accidents, particularly any that could cause an unacceptable release." (DOE/RL-96-0006, Section 4.1.1.2)

2.2.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph

2.2.2 Discussion

The provision of hazard elimination and protection shall be optimized by measures such as the choice of siting, proven conservative design and construction, a robust start-up testing program, operating requirements (i.e., clear definition of normal and abnormal operating conditions and maintenance activities).

Siting. The RPP-WTP site location will reduce the need to provide design measures to alleviate potentially hazardous conditions or to protect surrounding populations (for example, consideration of ground instability, river flooding, and hazards due to nearby industrial installations or activities) (Ref. 5.3).

Material at Risk. The RPP-WTP and its process design and administrative controls will minimize and control inventories of radioactive materials and their forms (Ref. 5.3).

Conservative Design. The RPP-WTP design will include conservative margins that allow flexibility of operations and maximize the time before requiring corrective actions. These margins will also take into consideration the potential degradation of elements and operational errors (Ref. 5.3).

The design shall address all identified hazards and hazardous situations and pursue methods for their prevention. The preferred means of prevention is to eliminate or reduce the severity of the hazard itself. According to the Implementation Guide on nonreactor facility safety, one objective of prevention as an element of defense in depth is to apply facility and process design and administrative controls to minimize and control inventories of radioactive materials and their forms (that is, minimize the material at risk) (Ref. 5.3).

Elimination or reduction of the hazard can be achieved by substituting less hazardous materials in processing, limiting the inventory of the material, etc. The design process must provide evidence through documentation that this option was considered and implemented to the maximum extent practicable. Where the hazard itself cannot be eliminated or reduced, controls shall be provided to reduce the likelihood of the hazard manifesting itself into an accident. The criterion for acceptability is discussed in Section 3.0. Where hazard elimination is not practicable, passive features are to be employed, since they are simple and have a high degree of reliability. Where this is not practicable, active protection will be proposed that has a degree of reliability and confidence commensurate with the potential hazard severity.

To illustrate the differences between hazard elimination and the provision of passive or active protection, consider the need for a cask lift using a crane. Elimination of the hazardous situation (inherent safety) is removal of the potential for raising a cask above its safe drop height by ensuring that the building dimensions physically prevent a lift above that height at all points of travel. If this were not practical, the provision of a physical stop would be passive protection to prevent a lift above the safe drop height. Active protection systems would include limit switches and braking systems. Procedures and operator training would ensure that the crane is handled and operated in a way that maximizes safety (e.g., check security of load, minimum lift height to confirm security, no challenge to engineered systems, and exclusion of personnel from load lifting area).

2.3 Control

"Normal operation, including anticipated operational occurrences, maintenance and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems and components important to safety is small." (DOE/RL-96-0006, Section 4.1.1.3)

2.3.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
4. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)

2.3.2 Discussion

The DOE Implementing Guidance for nonreactor facility safety provides two criteria related to the defense in depth sub-principle of control:

Critical safety functions. Design to provide multiple ways for safety functions to control processes, to maintain processes in a safe state, and to confine radioactivity when accidents could have the potential for significant [ ] radiological impact *to the public, facility workers or collocated workers* (Ref. 5.3).

Equipment and administrative controls. Include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3).

Normal operations, which include anticipated operational occurrences and maintenance and testing activities, shall be controlled so that facility and system parameters remain within their specified operating ranges and that the frequency of demands placed on SSCs for hazard prevention and mitigation is small.

This will be achieved by the choice of design that will:

1. Control key operating parameters such that facility operations remain within the safe operating envelope. Key operating parameters are those that define how the plant will be operated safely.
2. Maintain the safe operating envelope (e.g., a wide variation in operation conditions can be tolerated without entering into a potentially unsafe region).
3. Ensure that any failure mode would not move the facility or process toward a potentially unsafe region (i.e., fail to safe state).
4. Provide instrumentation and control features (e.g. temperature, pressure, radiation monitoring) which will warn of reduced margins of safety and, where appropriate, automatically return the process into the designated safe operating regime.
5. Achieve independence between SSCs credited for control of normal facility operations and those credited for prevention and mitigation of potential hazards.

For example, assume that the normal operating temperature range in an ion exchange column is set at 30 - 50 °C and that column temperatures above 80 °C lead to enhanced resin degradation and a potential explosion hazard. Engineered controls for maintaining that temperature within the normal operating limits (e.g., temperature control system) will be independent of that which would alert the operator and perform a preventative action (e.g., shut down process, increase cooling, etc.) in order that the hazard could not occur.

2.4 Mitigation

"The facility should be designed to retain the radioactive material through a conservatively designed confinement system for the entire range of events considered in the design basis. The confinement system should protect the workplace and the environment." (DOE/RL-96-0006, Section 4.1.1.4)

2.4.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02, see below)

2.4.2 Discussion

The purpose of mitigation is to ensure reduction of consequences from potential hazards and hazardous situations. One method of achieving this element of defense in depth is to ensure that suitable confinement of radioactive and hazardous material is maintained throughout normal operation and credible accident conditions. Confinement will be achieved by physical barriers and by other SSCs that either assure integrity of the physical barriers or minimize the quantity and characteristics of any hazardous material potentially releasable.

DOE Order 420.1, Chg 2, requires:

> "All nuclear facilities with uncontained radioactive materials (as opposed to material contained within drums, grout and vitrified materials) shall have means to confine them. Such confinement will act to minimize the spread of radioactive materials and the release of radioactive materials in facility effluents during normal operations and potential accidents. For a specific nuclear facility, the number and arrangement of confinement barriers and their required characteristics shall be determined on a case-by-case basis. Factors that shall be considered in confinement system design shall include type, quantity, form, and conditions for dispersing the material. Engineering evaluations, trade-offs, and experience shall be used to develop practical designs that achieve confinement system objectives. The adequacy of confinement systems to effectively perform the required functions shall be documented and accepted through the Safety Analysis Report." (Ref. 5.2)

The DOE nonreactor facility safety Implementation Guide defines confinement barriers to include primary confinement and secondary confinement. "Primary confinement provides confinement of hazardous material to the vicinity of its processing -- typically by means of piping, tanks, glove boxes, encapsulating material, etc., along with any offgas systems that control effluent from the primary confinement. As such, primary confinement addresses the preventive sub-principle of defense in depth, as well as mitigation. Secondary confinement consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area." [ ] (Ref. 5.3)

The RPP-WTP will provide physical barriers to confine radioactive material and thereby prevent uncontrolled releases. In general, multiple physical barriers - i.e., primary and secondary confinement - will be provided, especially for the most severe hazards and hazardous situations. Although RPP-WTP buildings will afford a tertiary confinement, as defined in the Implementation Guide, the RPP-WTP accident analysis will not take credit for holdup of radioactive materials by the buildings. The provision of multiple physical barriers will be tailored to the work and associated hazards, as discussed in Section 3.0.

The DOE nonreactor facility Implementation Guide (IG) suggests several industry consensus codes and standards for the design and construction of the SSCs comprising confinement, as follows: structures - IG subsection 5.2.1, ventilation systems - subsection 5.2.2.1, and process equipment - subsection 5.2.2.2. The specific standards for SSCs that implement mitigation with respect to SSCs comprising confinement are contained in the following Safety Criteria from the Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02):

- Structures - SC 4.1-2
- Ventilation systems - SC 4.4-6 through 4.4-8
- Process equipment - SC 4.2-1 through 4.2-3

2.5 Automatic Systems

"Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints." (DOE/RL-96-0006, Section 4.1.1.5)

2.5.1 Implementing Standards

1. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
2. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)
3. ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

2.5.2 Discussion

Automatic systems shall be provided to prevent the facility from entering into or remaining within an unsafe regime that may lead to the potential for radioactive or hazardous material release to workers, the public, or the environment, except as discussed below. The definition of the boundaries between safe and unsafe regimes will be determined as a result of detailed facility design, start-up, and testing activities. This will allow the derivation of the predetermined setpoints for safe facility operations. Automatic systems will be part of the overall suite of SSCs provided as part of the hazard control strategy. The determination of the need for automatic systems will be assessed as part of the determination of the overall hazards control strategy.

Means shall be provided to automatically initiate and control all protective actions except as justified below. The design of important to safety systems shall be such that the operator is not required to take any action prior to the time described below following the onset of any event (Based on IEEE Std 603-1991 - Ref. 5.11).

Credit for operator action may be permissible only if safety analysis demonstrates that the total time interval required to perform the operator action exceeds the time at which the limiting design requirement would be reached without operator action, in accordance with the methodology of ANSI/ANS-58.8-1994 (Ref. 5.7).

2.6 Human Aspects

"The human aspects of defense in depth should include a design for human factors, a quality assurance program, administrative controls, internal safety reviews, operating limits (Technical Safety Requirements), worker qualification and training, and the establishment of a safety/quality program." (DOE/RL-96-0006, Section 4.1.1.6)

2.6.1 Implementing Standards

1. IEEE Std 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12).
2. Implementing standards for the quality assurance program, administrative controls, internal safety reviews, operating limits (Technical Safety Requirements), worker qualification and training, and the establishment of a safety/quality program are contained in the Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), as discussed below.

2.6.2 Discussion

<u>Design for Human Factors</u>

The design shall apply human factors engineering (HFE) to address the ergonomic requirements of facility operations and maintenance of the RPP-WTP. The DOE nonreactor Implementation Guide recommends that the following human factor elements be considered: equipment labeling, workplace environment (temperature and humidity, lighting, noise, vibration, and aesthetics), human dimensions, operating panels and controls, component arrangement, warning and annunciator systems, and communication systems (Ref. 5.3).

The RPP-WTP design engineers, in consultation with operators, will apply these HFE elements in the design of important to safety SSCs to ensure that operational preferences are implemented. Human factors engineering specialists will provide support in the application of HFE.

Human factors engineering shall be conducted in accordance with IEEE Std 1023-1988 (Ref. 5.12), as discussed below. Selection of this subordinate standard comports with the nonreactor safety Implementation Guide (Ref. 5.3).

IEEE Std 1023-1988 was developed specifically for nuclear power generating stations. Therefore, this subordinate standard will be tailored to the work and hazards of the RPP-WTP as follows. The formal HFE process described in subsection 6.1.1 of IEEE Std 1023-1988 will be applied to the evaluation of hazards whose consequences fall into the two highest severity levels - SL-1 and SL-2, with the following clarification:

> The project does not plan on constructing a separate plant simulator or physical mockup. The RPP-WTP distributed control system (DCS) - including the main control room panels -- is a programmable computer system. The project envisions having the DCS built, delivered to the site and proof-tested with the aid of the facility operators well in advance of plant startup. Therefore, a dynamic simulation capability for personnel training will be provided for SSCs with significant human interfaces that involve complex and interactive processes (Ref. IEEE Std 1023-1988 §§ 6.1.1.12 and 6.1.1.18).

Although the structured HFE program outlined in subsection 6.1.1 of IEEE Std 1023-1988 will not be implemented for SL-3 and SL-4 events, the general HFE elements will be considered for all ITS SSCs, as committed above.

Similarly, formal consideration of the HFE techniques and methodologies recommended in Section 5 of IEEE Std 1023-1988 will be undertaken for hazards of severity levels SL-1 and SL-2. Certain of these techniques and methodologies may be utilized in the evaluation of SL-3 and SL-4 events in the context of the normal design and hazard assessment and control effort, as part of the integrated safety management process.

Quality Assurance Program

The *Safety Requirements Document Volume II* (24590-WTP-SRD-ESH-01-001-02) Safety Criteria 1.0-10 and Section 7.3 require the RPP-WTP contractor to establish and implement a Quality Assurance Program compliant with 10 CFR 830.120. This program is being implemented in accordance with the *Quality Assurance Manual* (24590-WTP-QAM-QA-01-001).

The *Quality Assurance Manual* (24590-WTP-QAM-QA-01-001) applies specifically to work performed on or for the RPP-WTP. The QAP is in conformance with 10 CFR 830.120 (Ref. 5.1) and with the top-level principles stated in DOE/RL-96-0006 (Ref. 5.4).

Administrative Controls

Administrative controls include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3).

The primary means of implementing defense in depth is through the provision of multiple physical barriers that maintain confinement. The output of the design process, through which hazards and hazardous situations are identified, control strategies implemented and standards defined will be a set of SSCs that achieve defense in depth. SSCs so identified will always be backed up by administrative controls such as procedures. Administrative controls that afford a measure of defense in depth will be developed prior to facility operations. For the purpose of protecting the public and collocated worker, administrative controls alone shall not be relied on for the implementation of defense in depth. Administrative controls alone may be credited as the controls that protect facility workers, when appropriate. In such cases, defense in depth is provided through other human aspects, such as worker qualification and training.

Internal Safety Reviews

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criterion 7.1-3, requires that the RPP-WTP contractor establish a safety framework and specifies requirements for the Internal Safety Oversight program consistent with Top-Level Principle 4.4.1, "Safety Review Organization". BNI has established a RPP-WTP Project Safety Committee (PSC) to provide an independent, interdisciplinary evaluation of matters related to nuclear, radiological, and process safety.

Operating Limits (Technical Safety Requirements)

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criterion 9.2-1, commits the RPP-WTP contractor to prepare, submit for approval, and operate the facility in accordance with Technical Safety Requirements (TSRs). SCs 9.2-2 through 9.2-6 provide the safety criteria for the bases and contents, updating, submission for regulatory approval, and maintenance of TSRs.

As part of hazard evaluation, the role of the operator in the development of a potential hazard will be identified and reliability assessed. Human factors specialists in the multidisciplinary team will support this evaluation. The results of the assessment will be incorporated into administrative controls such as operating procedures and TSRs.

Worker Qualification and Training

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Section 7.2, commits the RPP-WTP contractor to establish and implement a training program. Consistent with Top-Level Principles 4.3.4.1, "Personnel Training", 4.3.4.2, "Training Programs", and 5.2.4, "Process Safety - Training," SRD Volume II, Section 7 requires that the program address:

- continual training - SC 7.2-1, 7.2-3, 7.3-3
- qualification of personnel - SC 7.3-3
- records of training status - SC 7.2-4
- establishment of written procedures/instructions - SC 7.2-2, 7.2-5

Establishment of a Safety/Quality Program

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criteria 1.0-1, requires the use of a comprehensive safety management program consistent with Top-Level Principle 5.1.1, "Process Safety Management", and 5.1.2, "Process Safety Objective". Safety Criterion 7.1-3 requires a safety framework be established to implement this Program consistent with Top-Level Principle 4.1.4.1, "Safety/Quality Culture".

Establishment of a Quality Program is discussed above under the heading, "Quality Assurance Program".

3.0 Determination of SSCs for the Implementation of Defense in Depth

The standards for prevention, control, and human aspects in Sections 2.2, 2.3, and 2.6 are primarily concerned with defense in depth sub-principles that minimize the potential of hazard initiation. In evaluating accidents that are postulated to occur despite implementation of preventive, control and human aspects, the sub-principles of mitigation and automatic systems must be considered.

The Implementing Standard for Safety Standards and Requirements Identification describes the process by which hazards and hazardous situations are identified and evaluated to determine hazard control strategies. Use of this Implementing Standard ensures that the defense in depth sub-principles are accounted for in the process of determining hazard control strategies. That process will identify SSCs that perform defense in depth as part of their safety function. The administrative controls that back up these SSCs will be developed prior to the introduction of hazardous materials into the facility.

Table 1 is the standard for implementing defense in depth by SSCs as part of the hazard control strategy; it defines the minimum number of SSCs and associated engineering requirements for the control of hazards of a particular severity.

Table 1 will be used in conjunction with the guidance in Section 2.0 to ensure that the preferred control solution addresses the strategies that protect the public and collocated workers; such SSCs will always be backed up by the human aspects of defense in depth discussed in Section 2.6.

The table lists the number and attributes of the physical barriers, as well as the application of the single failure criterion to SSCs that are required to adequately implement defense in depth for a given control strategy. Confirmation of the adequacy of implementation is achieved by meeting the numerical guidance stated in the third column. Consistent with the defense in depth sub-principles in Section 2.0, the control strategy should emphasize passive SSCs over active SSCs.

Hazard severities and target frequencies are the means to achieve adequate defense in depth in accordance with the tailored approach mandated by RL/REG 98-17, "Regulatory Unit Position on Tailoring for Safety."

1st Column - SL (Severity Level)

Determination of hazard severity level is based on an assessment of unmitigated consequences. Severity levels are defined as SL-1 to SL-4, with SL-1 having the highest consequences.

2nd Column - Control Options for Implementation of Defense in Depth

A graded approach is reflected in the configuration requirements against each hazard severity level. The requirements are more stringent for defense in depth implementation for hazards of greater severity than for those of lesser severity.

Implementation of defense in depth requires that the single failure criterion be applied in a tailored fashion. For SL-1, application of the single failure criterion is mandatory. For SL-2, the single failure criterion shall be considered; that is, an objective assessment must be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. The single failure criterion is discussed in Section 2.1.

In addition to the single failure criteria in Table 1, diversity may also be implemented in the control strategy where hazards assessment reveals a common mode failure concern (see the Implementing Standard for Safety Standards and Requirements Identification, SRD Vol. II, Appendix A).

Implementation of defense in depth also requires that the provision of physical barriers be applied in a tailored fashion. In Table 1, provision of physical barriers refers to those that provide confinement against the release of hazardous materials, as opposed to barriers that protect against direct radiation. For SL-1 and SL-2, two or more independent physical barriers are required. For SL-3, at least one physical barrier shall be provided, and two or more independent physical barriers shall be considered; that is, an objective assessment must be performed to determine the extent to which physical barriers will be incorporated by the design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. For SL-4, physical design features and/or administrative controls per 10CFR 835.1001 shall be provided.

The graded approach is also reflected in the degree of confidence required commensurate with the hazard severity. The confidence is based on the standards and other attributes applicable to the particular control strategy. The Implementing Standard for Safety Standards and Requirements Identification describes selection of standards and other attributes applicable to control strategies.

3rd Column - Target Frequency (yr^{-1})

This column lists the target frequencies for each hazard severity level. The hazard severity level is a measure of the consequence from an unmitigated event - that is, an event in which both SSCs that prevent the accident and SSCs that mitigate the accident fail. After the preferred hazard control strategy has been identified, the event frequency - i.e., the product of the frequency of the initiating event and the probability that the control strategy will fail given the initiating event - will be conservatively estimated. (No credit is taken for administrative controls in calculating the initiating event frequency.) Verifying that the event frequency is less than the target frequency will provide confirmation that the chosen control strategy includes sufficient SSCs to adequately implement defense in depth in a graded approach.

The demonstration of having met the target frequencies may be based on either numerical analysis or engineering judgment. When appropriate, administrative controls alone may be credited as the controls that protect facility workers. The hazard assessment and control team shall assess the confidence in the frequency so determined, applying greater conservatism where engineering judgment is employed.

Table 1. Implementation of Defense in Depth by SSCs.

Severity Level	Control Options for Implementation of Defense in Depth	Target Frequency (yr^{-1})
SL-1	Two or more independent physical barriers. The single failure criterion shall be applied.	$< 10^{-6}$
SL-2	Two or more independent physical barriers. The single failure criterion shall be considered.	$< 10^{-4}$
SL-3	At least one physical barrier shall be provided. Two or more independent physical barriers shall be considered.	$< 10^{-2}$
SL-4	Physical design features and/or administrative controls per 10 CFR 835.1001	$< 10^{-1}$

4.0 Definitions

Definitions of the following terms were obtained from the referenced consensus standards. Minor wording differences among multiple references are ignored. In some cases, the definition of a term given in the referenced consensus standard has been tailored to the relative risks of the RPP-WTP and its anticipated associated hazards. Other wording differences in the definitions below from the cited consensus standards have been made to preserve consistency with terminology in other RPP-WTP safety documentation. Such differences are identified by presenting added words in Italics and by inserting double-brackets where words have been removed. Citation of a definition from a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

Active component [SSC]. A component in which mechanical movement must occur to accomplish the [ ] safety function of the component (Ref. 5.5, 5.6)

Active failure. A malfunction, excluding passive failures, of a component that relies on mechanical movement to complete its intended [ ] safety function upon demand

Examples of active failures include the failure of a valve or check valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start.

Spurious action of a powered component originating within its actuation or control system shall be regarded as an active failure unless the specific design features or operating restrictions preclude such spurious action. An example is the unintended energization of a powered valve to open or close (Ref. 5.5, 5.6, 5.8).

Administrative controls. Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of the facility.

Barrier. A control that has the function of maintaining confinement, that is preventing or mitigating the release of radioactive or hazardous material to the worker, public or the environment. This control can be an SSC that provides a physical barrier (e.g. vessel, shielding, and filtration) or an administrative control (e.g. training and procedures), which supplements the physical barriers.

Common cause failure. Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures (Ref. 5.4).

Common mode failure. Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation (Ref. 5.4).

Confinement. Physical barrier that prevents or mitigates the release of radioactive or hazardous material to the worker, public or the environment. The DOE nonreactor facility safety Implementation Guide identifies three kinds of confinement barriers - primary confinement, secondary confinement, and tertiary confinement (Ref. 5.3).

Control strategy. A set of generally-described provisions (barriers, dilution/dispersal, physical limitations on material quantities, administrative material controls, confinement, ventilation of flammable gas, etc.) and/or approaches (defense in depth, use of passive features, prevention, mitigation, etc.) which are intended to assure adequate control of a specific hazard and associated accidents in the context of the work (Ref. 5.4).

Defense in depth. The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or the environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualifications and training and safety program. Design provisions including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public or the environment (Ref. 5.4).

Design Basis Events. Postulated events providing bounding conditions for establishing the performance requirements of structures, systems and components that are necessary to: 1) ensure the integrity of the safety boundaries protecting the worker; 2) place and maintain the facility in a safe state indefinitely; or 3) prevent or mitigate the event consequences so that the radiological exposures to the general public or the workers would not exceed appropriate limits. The Design Basis Events also establish the performance requirements of the structures, systems, and components whose failure under Design Basis Event conditions could adversely affect any of the above functions (Ref. 5.4).

Detectable failures. [The following definition is considered to be specific to electrical, instrumentation and control systems.]

> Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication (Ref. 5.9).

Diversity. Use of different technologies, equipment, or design methods to perform a common function with the intent to minimize common cause failures (Ref. 5.13).

Engineered feature. A structure, system or component that contributes to the safe operation of the facility (Ref. 5.14).

Event. A condition that deviates from normal operation, i.e., an initiating occurrence plus single failure or coincident occurrence combination (Ref. 5.5, 5.6).

External Event. An event external to the RPP-WTP caused by (1) a natural hazard (e.g., earthquake, flood, lightning, or range fire) or (2) a human-induced event (e.g., transportation or nearby industrial activity).

Human factors engineering (HFE). An interdisciplinary science and technology concerned with the process of designing for human use (Ref. 5.12).

Important to Safety. Structures, systems and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems and components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems and components should be considered for inclusion within this definition (Ref. 5.4).

Independence. The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable (Ref. 5.10).

Initiating occurrence/event. A single occurrence and its consequential effects that place the plant or some portion of the plant in an off-normal condition. An initiating occurrence/event is not the single failure defined elsewhere herein. An initiating occurrence can be *an internal event or an external event* (Ref. 5.5, 5.6, 5.8).

The first event in an event sequence. Can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident (Ref. 5.15).

Internal Event. An occurrence related to structure, system, and component performance or human action, or an occurrence external to the system but within the RPP-WTP that causes upset of a structure, system, or component.

Limiting design requirements. The limiting value of a design parameter that ensures that the consequences of any event do not result in:

- Violation of plant nuclear safety criteria, including off-site radiological dose criteria, or
- Unacceptable degradation of plant components that are required to mitigate the consequences of an event.

(A single event may have more than one limiting design requirement.) (Ref. 5.7)

Long term. *For fluid systems*, the long term is defined as that period of *important to safety* fluid system operation following the short term during which the safety function of the system is required (Ref. 5.8).

Passive component. A component that is not an active component (Ref. 5.5, 5.6).

Passive failure. The blockage of a process flow path or failure of a component to maintain its structural integrity or stability, such that it cannot provide its intended [ ] safety function upon demand (Ref. 5.5, 5.6, 5.8).

Primary confinement. Provides confinement of hazardous material to the vicinity of its processing. This confinement is typically provided by piping, tanks, glove boxes, encapsulating material, and the like, along with any offgas systems that control effluent from the primary confinement (Ref. 5.3).

Redundant equipment or system. A system or component that duplicates the essential functions of another system or component to the extent that either may perform the required function, regardless of the state of operation or failure of the other (Ref. 5.9, 5.10).

Safety function. Any function that is necessary to ensure: 1) the integrity of the boundaries retaining the radioactive materials; 2) the capability to place and maintain the facility in a safe state; or 3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits (Ref. 5.4).

Secondary confinement. Consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area. Except in the case of housing glove-box operations, the area inside this barrier is usually unoccupied (e.g., canyons, hot cells); it provides protection for operating personnel (Ref. 5.3).

Shall, should and may. The word “shall” is used to denote a requirement; the word “should” is used to denote a recommendation; and the word “may” is used to denote permission, neither a requirement nor a recommendation (Ref. 5.5, 5.6, 5.8).

The word “shall” denotes actions that must be performed… The word “should” is used to indicate recommended practice (Ref. 5.3, based on DOE-STD-1075-94).

Shall [be] consider[ed]. An objective assessment must be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. (Ref. 5.16).

Short term. *For fluid systems*, the short term is defined as that period of operation up to 24 hours following an initiating event [ ] (Ref. 5.8).

Single failure. A random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended [ ] safety function(s) (Ref. 5.5, 5.6).

Single failure criterion. [Two definitions are provided below. The following definition applies to fluid (i.e., liquid and gas) systems.]

> Fluid [ ] systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly), nor (2) a single failure of any passive component (assuming active components function properly) results in a loss of the capability of the system to perform its [ ] safety function (Ref. 5.5, 5.6).

[The following statement of the "single failure criterion" applies to electrical and instrumentation and control systems.]

> The *important to* safety systems shall perform all required safety functions for a design basis event in the presence of the following:
>
> 1. Any single detectable failure within the *important to* safety systems concurrent with all identifiable but non-detectable failures
> 2. All failures caused by the single failure
> 3. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function
>
> The single failure could occur prior to, or at any time during, the design basis event for which the *important to* safety system is required to function (Ref. 5.9).

5.0 References

5.1 10 CFR 830.120, Quality Assurance Requirements

5.2 DOE O 420.1, Facility Safety, Chg 2, 10/24/96

5.3 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria, Rev. G (Draft), September 1995

5.4 DOE/RL-96-0006, Revision 1, Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors

5.5 ANSI/ANS-51.1-1983, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. American Nuclear Society

5.6 ANSI/ANS-52.1-1983, Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants. American Nuclear Society

5.7 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions. American Nuclear Society

5.8 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems. American Nuclear Society

5.9 IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems. IEEE Power Engineering Society

5.10 IEEE Std 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits. IEEE Power Engineering Society

5.11 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. IEEE Power Engineering Society

5.12 IEEE Std 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.

5.13 ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries. Instrument Society of America.

5.14 Integrated Safety Management Plan. 24590-WTP-ISMP-ESH-01-001. Bechtel National, Inc., Richland, WA

5.15 Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples. Center for Process Chemical Safety, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1992.

5.16 DOE O 6430.1A, General Design Criteria, 6 April 1989

6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth

The following subsections summarize the RPP-WTP contractor's tailoring of the consensus standards invoked by this Implementing Standard for Defense in Depth.

6.1 DOE O 420.1, Facility Safety (Ref. 5.2)

Terminology

- Section 4.1.1.2, 1st paragraph, last sentence: Phrase "…workers, including those at adjacent facilities…" is interpreted for RPP-WTP to mean "…workers and collocated workers…"

Applicability

- The only portion of DOE O 420.1 that is being invoked by this Implementing Standard for Defense in Depth is Section 4.1.1.2, the first three paragraphs.

6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3)

Terminology

- By virtue of cross-references within the DOE Implementation Guide (IG), reference is made to "safety class" and "safety significant" SSCs. The RPP-WTP project uses the term "important to safety", which encompasses both "safety class" and "safety significant".
- "Critical safety function" in the DOE IG is interpreted to more broadly read "…significant public, worker and collocated worker impact".

Applicability

- The only portion of the DOE "420.X" Implementation Guide that is being invoked by this Implementing Standard for Defense in Depth is Section 2.3, except the last paragraph.
- Section 2.3 of the DOE IG contains internal cross-references to subsections 5.2.1, 5.2.2.1 and 5.2.2.2, which list typical codes for structures, ventilation systems, and process equipment that provide a confinement function. Section 2.4.2 of this Implementing Standard lists the SRD Safety Criteria that will be applied to SSCs comprising confinement.
- Section 2.3 of the DOE IG contains an internal cross-reference to subsection 5.2.1, which further cites section 4.4 of DOE O 420.1 and section 3.3 of the DOE IG for criteria for natural phenomena hazards (NPH). For the RPP-WTP, NPH criteria are provided in SRD Safety Criteria SC 4.1-3 and SC 4.1-4.

6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

Terminology

- "Safety-related" is interpreted for RPP-WTP to mean "important to safety" or "ITS".
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function" as defined in DOE/RL-96-0006, Rev. 1.

Non-Applicability

- Assumption (1) of section 1.3 does not apply. Single failure criteria for the RPP-WTP project are given in the consensus standards invoked and tailored by this Implementing Standard (ANSI/ANS-58.9-1981 and IEEE 379-1994).
- Assumption (4) of section 1.3 does not apply. The operators will be qualified in accordance with the RPP-WTP training program, per Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Section 7.2.
- "Automatic reactor trip…" does not apply.

6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)

Terminology

- "Containment" or "containment vessel" is interpreted to mean "confinement".
- "Seismic Category I standards" is interpreted as seismic requirements for a SSC with a seismic safety function per SRD Volume II (24590-WTP-SRD-ESH-01-001-02) Safety Criterion 4.1-3 for the RPP-WTP.
- "Safety related" is interpreted for RPP-WTP to mean "important to safety" or "ITS". Conversely, "non-safety-related" means "non-ITS".
- "Technical specification(s)" is interpreted to mean "Technical Safety Requirements" or "TSR(s)".
- "Condition I" is interpreted for RPP-WTP to mean "normal operation".
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function" as defined in DOE/RL-96-0006, Rev. 1.
- In definition of "single failure", reference [1] does not apply to RPP-WTP.
- Safety classes 1, 2, and 3 (section 4.5) are interpreted to be important to safety systems.

Non-Applicability

- For RPP-WTP, the need for emergency onsite power will be ascertained in accordance with the DOE/RL-96-0004 process as part of determining hazard control strategies.
- In the definition of "short term" (section 2), everything after "…up to 24 hours following an initiating event" applies to nuclear power reactor plants and is therefore not applicable to RPP-WTP.
- Sections 3.1 through 3.3 of ANSI/ANS 58.9 are not applicable to the RPP-WTP. Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Reactor-specific regulations (e.g., 10 CFR 50 Appendix A) are not applicable to RPP-WTP (see Section 1, 1st paragraph).
- References to a reactor "unit", "safe shutdown", and "loss of coolant accident" are nuclear reactor plant-specific and, therefore, do not apply to RPP-WTP.
- Sections 3.1 through 3.3 are reactor-specific and do not apply to RPP-WTP.

6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

Terminology

- BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:
  - Common-cause failure
  - Design basis events
  - Safety function
- "Safety system" is interpreted for RPP-WTP to mean "important to safety system". Consequently, "important to safety system" is interpreted to mean a system that performs a safety function, as defined in DOE/RL-96-0006.
- "Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.

Applicability

- Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Nuclear reactor plant-specific terms such as reactor "unit", "reactor trip system" power, control rods, "safety injection", "core spray", and "low pressure coolant injection" do not apply to RPP-WTP.

6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)

Terminology

- The definition of "administrative controls" in section 2 of the consensus standard is understood as being consistent with the definition given in section 4.0 of this Implementing Standard.
- The definition of "Class 1E" is interpreted for the RPP-WTP as follows: "The classification of the electric equipment and systems that perform a safety function." The note following the definition of "Class 1E" in the consensus standard is retained for RPP-WTP.
- BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:
  - Design basis events
  - Safety function
- "Safety system" is interpreted for RPP-WTP to mean "important to safety system". Consequently, "important to safety system" is interpreted to mean a system that performs a safety function, as defined in DOE/RL-96-0006.
- "Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.
- "Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.

Non-Applicability

- Nuclear reactor plant-specific terms such as reactor "unit", "emergency reactor shutdown", "reactor heat removal", do not apply to RPP-WTP.

6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12)

Terminology

- "Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.

Non-Applicability

- Application of the formal human factors engineering process described in subsection 6.1.1 of IEEE Std 1023-1988 is tailored to the work and hazards presented by the RPP-WTP in subsection 2.6.2 of this Implementing Standard.

- Section 6.1.1.12 and 6.1.1.18 of IEEE Standard 1023-1998 recommends the use of a separate plant simulator or physical mockup for human factors engineering. As discussed in subsection 2.6.2 of this Implementing Standard, the RPP-WTP contractor does not currently plan to construct a separate plant simulator or physical mockup and these sections are, therefore, not applicable to RPP-WTP.

6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13)

Terminology

- The definition of "common-cause failure" given in DOE/RL-96-0006 is used, rather than that in section 3 of the consensus standard.
- "Safety Instrumented System (SIS)" is interpreted to refer to any instrumentation and control system in the RPP-WTP that is important to safety, as defined in DOE/RL-96-0006.

Appendix C

Implementing Standards

CONTENTS

Section Implementing Standard **Page**

1.0 ISO 10007, Quality Management - Guidelines for Configuration Management C-1
2.0 DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities" C-3
3.0 ANSI/AISC N690, "Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities" C-12
4.0 DOE G-420.1/G-440.1, Implementation Guide for Use with DOE Orders 420.1 and 440.1, Fire Safety Program C-13
5.0 DOE-STD-1066-97, Fire Protection Design Criteria C-14
6.0 NFPA 801, Standard for Facilities Handling Radioactive Materials C-16

1.0 ISO 10007, Quality Management - Guidelines for Configuration Management

Revision: First Edition, April 15, 1995
Sponsoring Organization: International Organization for Standardization

RPP-WTP Specific Tailoring

The following tailoring of ISO 10007 is required for use by the RPP-WTP contractor as an Implementing Standard for Configuration Management.

Page 1, Section 1 Scope

Second paragraph, last sentence. Replace this sentence with:

"For RPP-WTP ISO 10007 amplifies on the configuration management elements found in the Quality Assurance Program, BNFL-5193-QAP-01."

Justification: For RPP-WTP the approved QAP defines the quality management and quality system elements.

Page 1, Section 2 Normative References

Delete reference to the ISO 10011 series of standards.

Justification: As discussed for Section 8, for RPP-WTP the approved QAP defines the principles, criteria, and practices for the configuration management system audit.

Page 7, Section 7.7 Configuration Management Plant (CMP)

Delete second paragraph

Justification: This paragraph addresses activities outside the RPP-WTP project workscope or control (i.e., multiple projects, multi-level contracts, and customer configuration management plans).

Page 8, Section 8 Configuration Management System Audit

Revise the last paragraph to read:

"Principles, criteria, and practices of the CM system audit should comply to the RPP-WTP QAPIP."

Justification: For RPP-WTP the approved QAP defines the principles, criteria, and practices for the conduct of audits and self-assessments.

Page 11 and 12, Annex B

Delete.

Justification: Although provided only as information, as noted in Section 1 above, the ISO 9000 Series of Standards are not being implemented at RPP-WTP and this Annex is therefore removed to reduce potential confusion to non-applicable cross references.

2.0 DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities"

Revision: Change Notice #1 dated 1/96 and DOE Newsletter dated 1/22/98 (Interim Advisory on Straight Winds and Tornados)

Sponsoring Organization: DOE

RPP-WTP Specific Tailoring

The following tailoring of DOE-STD-1020-94 is required for use by the RPP-WTP contractor as an Implementing Standard for seismic analysis and design.

Page 1-6, Section 1.3 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 2-1, Section 2.2 General Approach for Seismic Design and Evaluation

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page 2-6, Section 2.3 Seismic Design and Evaluation of Structures, Systems, and Components

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 2-8, Section 2.3.1 Performance Category 1 and 2 Structures, Systems, and Components

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 2-12, Section 2.3.2 Performance Category 3 and 4 Structures, Systems, and Components

Disregard the requirements for PC-4 SSCs.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use ACI 349 for design of reinforced concrete in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Use ANSI/AISC N690 for design of structural steel in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Page 2-15, Section 2.3.3 Damping Values for Performance Category 3 and 4 Structures, Systems, and Components

Use ASME Code Case N-411 damping value for piping in lieu of those shown in Table 2-3.

Justification: This value is acceptable to the NRC for nuclear power plants.

Page 2-18, Section 2.4.1 Equipment and Distribution Systems

Perform seismic design of PC-1 and -2 elements of structures and equipment per the provisions of 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 2-22, Section 2.4.2 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 2-24, Section 2.5 Summary of Seismic Provisions

Disregard the requirements for PC-4 SSCs.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use the seismic provisions in Table 2-5 concerning PC-3 SSCs except that the structural capacity is to be based on code ultimate strength or allowable behavior level.

Justification: Limit-state level method of determining the structural capacity is more appropriate for evaluation of existing facilities (the RPP-WTP is a new facility).

Page 3-1, Section 3.1 Introduction

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 3-2, Section 3.2 Wind Design Criteria

Use peak gust speed values contained in Attachment "A" of DOE Interim Advisory dated 1/22/98 in lieu of fastest-mile wind speeds shown in Table 3-2; also, per DOE Interim Advisory, use an importance factor for PC-2 SSCs of 1.0 in lieu of 1.07 indicated in Table 3-1.

Justification: The Newsletter was issued by DOE as an interim measure for use with DOE-STD-1020-94 until such time as the standard is revised.

Page 3-5, Section 3.2.1 Performance Category 1

Design structural steel PC-1 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred to the UBC because it is a national consensus code.

Design reinforced concrete PC-1 structures per ACI 318-99.

Justification: The ACI 318 code is preferred to the UBC because it is a national consensus code.

Page 3-6, Section 3.2.2 Performance Category 2

Design structural steel PC-2 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred to the UBC because it is a national consensus code.

Design reinforced concrete PC-2 structures per ACI 318-99.

Justification: The ACI 318 code is preferred to the UBC because it is a national consensus code.

Page 3-6, Section 3.2.3 Performance Category 3

Design structural steel PC-3 structures per ANSI/AISC N690-94.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Design reinforced concrete PC-3 structures per ACI 349-97.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Disregard requirements for tornado design.

Justification: Tornado is not a credible NPH at the RPP-WTP site.

Page 3-11, Section 3.2.4 Performance Category 4

Delete this section.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Page 3-13, Section 3.3 Evaluation of Existing SSCs

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 4-1, Section 4.0 Flood Design and Evaluation Criteria

Disregard criteria for the design of SSCs for river flooding.

Justification: River flooding is not a credible NPH at the RPP-WTP site, and only the criteria dealing with local precipitation that affects roof design and site drainage are applicable to the RPP-WTP design.

Page 4-4, Section 4.1.2 Flood Evaluation Process

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 4-12, Section 4.2.4 Performance Category 4

Delete this section.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Page 4-13, Section 4.3.3 Site Drainage and Roof Design

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 4-15, Section 4.4 Considerations for Existing Construction

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 4-16, Section 4.5 Probabilistic Flood Risk Assessment

Do not perform a probabilistic flood risk assessment of the RPP-WTP site.

Justification: UCRL-21069, "Probabilistic Flood Hazard Assessment for the N Reactor, Hanford, Washington", July 1988, contains a probabilistic flood risk assessment of the N reactor site. The RPP-WTP site is close to the N Reactor site (about 10 miles away) and further away from the Columbia River. Therefore, the N Reactor flood assessment may be used and no assessment of the RPP-WTP site is required.

Page B-4, App. B, Section B.2 Graded Approach, Performance Goals, and Performance Categories

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page B-8, App. B, Section B.3 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page C-1, App. C, Section C.1 Introduction

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page C-19, App. C, Section C.3.2 Earthquake Ground Motion Response Spectra

Disregard Section C.3.2.1 discussion and Table C-4. Follow 1997 UBC for the RPP-WTP design.

Justification: Section C.3.2.1 discussion and Table C-4 are based on 1994 UBC; the 1997 UBC is more current.

Page C-27, App. C, Section C.4 Evaluation of Seismic Demand (Response)

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page C-29, App. C, Section C.4.1 Dynamic Seismic Analysis

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page C-31, App. C, Section C.4.2 Static Force Method of Seismic Analysis

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page C-32, App. C, Section C.4.3 Soil-Structure Interaction

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page C-38, App. C, Section C.4.4 Analytical Treatment of Energy Dissipation and Absorption

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Page C-52, App. C, Section C.5.1 Capacity Approach

Use ACI 349 for design of reinforced concrete in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Use ANSI/AISC N690 for design of structural steel in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Page C-62, App. C, Section C.7 Special Considerations for Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page C-66, App. C, Section C.9 Alternate Seismic Mitigation Measures

Delete this section.

Justification: Seismic base isolation is not planned to be used in the RPP-WTP design.

Page D-3, App. D, Section D.3 Load Combinations

Design structural steel PC-1 and PC-2 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred because it is a national consensus code.

Design reinforced concrete PC-1 and PC-2 structures per ACI 318-99.

Justification: The ACI 318 code is preferred because it is a national consensus code.

Design structural steel PC-3 SSCs structures per ANSI/AISC N690-94.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Design reinforced concrete PC-3 SSCs structures per ACI 349-97

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

3.0 ANSI/AISC N690, "Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities"

Revision: 1994

Sponsoring Organization: American National Standards Institute/American Institute of Steel Construction

RPP-WTP Specific Tailoring

The following tailoring of ANSI/AISC N690 is required for use by the RPP-WTP contractor as an Implementing Standard for structural design.

Page 22, Section Q1.5.7.1 Primary Stresses

Revise the stress limit coefficients for compression in Table Q1.5.7.1 as follows:

- 1.3 instead of 1.5 [stated in footnote (c)] in load combinations 2, 5, and 6
- 1.4 instead of 1.6 in load combinations 7, 8, and 9
- 1.6 instead of 1.7 in load combination 11

Justification: These changes are made for consistency with the NRC requirements of Appendix F of Section 3.8.4 of NUREG-0800 (Draft Rev. 2).

4.0 DOE G-420.1/G-440.1, Implementation Guide for Use with DOE Orders 420.1 and 440.1, Fire Safety Program*

Revision: September 30, 1995

Sponsoring Organization: U. S. Department of Energy

RPP-WTP Specific Tailoring

The following tailoring of DOE G-420.1/G-440.1 is required for use by the RPP-WTP Project as an implementing standard for fire safety.

Section III.5.0

Add the following words at the end of the paragraph: "The applicable building code for the RPP-WTP Project is the 1997 Uniform Building Code (UBC)."

Justification: To clarify that the code in effect at the time that facility design commenced was the 1997 UBC.

Section III.6.3

Revise to read "Automatic fire extinguishing systems in all areas subject to loss of safety class systems, significant life safety hazards, or unacceptable program interruption. The FHA may justify the omission of such systems based on safety considerations as approved by the AHJ.

Justification: The addition is consistent with governing Safety Criterion 4.5-4, which requires automatic fire suppression "unless the Fire Hazards Analysis dictates otherwise". It is also consistent with the DOE equivalency concept described in DOE G-420.1/G-440.1 Section II.

Section IV.4.5

Change "Description of critical process equipment" to "Identification of Important-To-Safety Equipment".

Justification: The term "critical process equipment" is not well defined for the RPP-WTP Project. By contrast the term "Important-to-Safety" is defined by the DOE regulatory documents, such as DOE/RL-96-0004. Identification of Important-to-Safety equipment is more meaningful and is consistent with the CAR Guidance (RL/REG-99-05).

5.0 DOE-STD-1066-97, Fire Protection Design Criteria

Revision: March 1997

Sponsoring Organization: U. S. Department of Energy

RPP-WTP Specific Tailoring

The following tailoring of DOE-STD-1066-97 is required for use by the RPP-WTP Project as an implementing standard for fire safety.

Section 9.5.1

Add the following words: "The fire resistance of special or unique penetration assemblies, such as lead glass windows and shield wall penetrations, may be based on past qualification testing or an equivalency evaluation."

Justification: The RPP-WTP facility is expected to have unique penetration configurations that may be impractical to test. This change clarifies that alternate approaches that provide a comparable level of safety, as described in Section 1 of DOE-Std-1066-97, may be used.

Section 10.4

Add the following words: "The 75-foot travel distance may be exceeded in areas not normally occupied by personnel, where plant equipment alone is located".

Justification: If an area is not normally occupied an accidental breach of a primary confinement system cannot expose personnel to radioactive material.

Section 10.6.3:

Delete the statement that: "In addition, for explosives environments, exits should reflect the criteria contained in the DOE Explosives Safety Manual (DOE M 440.1-1)."

Justification: The DOE Explosives Safety Manual applies to environments involving munitions, and is not applicable to the RPP-WTP.

Section 11.4

Revise this section to read: "Where required by the SAR, critical facilities should be served by dedicated, redundant electric power services. External to the buildings served, the two services should be separated by 4-hour fire-rated construction and should be served from separate sources.

Justification: The term "power services" is more consistent with the sentence that follows. The changes clarify that the requirement applies to site power supplies, not to cable routing within the buildings served.

Section 12.4

Delete this section.

Justification: This section is not applicable because there will be no gas-fired process furnaces in the RPP-WTP.

Section 13

Delete all except Subsection 13.1

Justification: The RPP-WTP is not a Plutonium Processing and Handling Facility, a Plutonium Storage Facility, an Enriched Uranium Storage Facility, a Uranium Processing and Handling Facility, a Fuel Reprocessing Facility, or a Uranium Conversion and Recovery Facility.

6.0 NFPA 801, Standard for Facilities Handling Radioactive Materials

Revision: 1995 edition

Sponsoring Organization: National Fire Protection Association

RPP-WTP Specific Tailoring

The following tailoring of NFPA 801-95 is required for use by the RPP-WTP project as an implementing standard for fire safety.

Section 3-8

Replace entire section with the text of the same section from the 1998 version of NFPA 801.

Justification: The NFPA standard was revised in recognition of the impracticality of using only noncombustible surface finishes in areas processing or storing radioactive materials. Conformance with the revised standard will permit the use of limited combustible interior finishes.

Section 6.1.1

Change the code edition for NFPA 70 from 1993 to 1996 and the code edition for NFPA 780 from 1992 to 1995.

Justification: SRD safety criteria 4.3-2 and 4.4-12 reference these more recent editions of NFPA 70 and NFPA 780 as implementing standards. This change resolves the conflict with NFPA 801.

Appendix D

Radiological Exposure Standards for the RPP-WTP Project

CONTENTS

1.0 Introduction and Purpose D-1
2.0 Exposure Standards for Facility and Collocated Workers D-2
3.0 Development of the BNI Approach to Compliance with Table 1 of DOE/RL-96-0006 ..... D-5
3.1 Estimated Frequency of Occurrence D-5
3.2 Normal Events/Public and Workers Exposure Standards D-5
3.3 Anticipated Events/Worker and Collocated Worker Exposure Standards D-6
3.4 Extremely Unlikely Events/Public Exposure Standard D-7
3.5 Location of Receptors D-7
3.5.1 Facility Worker D-7
3.5.2 Collocated Worker D-9
3.5.3 Public D-9
4.0 References D-12

1.0 Introduction and Purpose

This attachment to the SRD originally was issued as a stand-alone document (BNFL-5193-RES-01, Rev. 0, dated August 28, 1997). It has been incorporated into the SRD because it provides both background information and the basis for the radiological exposure standards reflected in the SRD Safety Criteria. In addition, it has been updated to reflect responses to DOE questions on the Standards Approval Package.

This document is the Radiation Exposure Standard for Workers Under Accident Conditions, which is a radiological safety deliverable. This document is used during the process hazards analysis (PHA) and accident analysis to ensure worker safety through identification of the need for accident prevention and mitigation features that provide worker protection against radiological and nuclear hazards. In this document, where unmodified reference is made to workers, it applies collectively to facility workers and collocated workers as defined in Sections 3.5.1 and 3.5.2 below.

The U.S. Department of Energy (DOE), in DOE/RL-96-0006, Revision 0, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, (DOE-RL 1996), provides Table 1, "Dose Standards Above Normal Background". In Table 1 (referred to as DOE Table 1), there are entries labeled, "To be derived", for which the contractor is to propose specific exposure standards for both facility workers and collocated workers for the following events:

- **Unlikely Events**: events that are not expected but may occur during the lifetime of the facility in the range of frequency between 10^{-2}/yr and 10^{-4}/yr (between once in 100 years and once in 10,000 years)
- **Extremely Unlikely Events**: events that are not expected to occur during the lifetime of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material. Extremely unlikely events are in the range of frequency between 10^{-4}/yr and 10^{-6}/yr (between once in 10,000 years and once in 1 million years).

This document provides the required exposure standards and the bases for their selection. In addition, this document presents the approach for complying with DOE Table 1. The individual elements of this approach, as shown in Table 2-1 of SRD Safety Criterion 2.0-1 (referred to as Table 2-1), are conservative based on the requirements of the contract and, as such, satisfy the contract. For completeness, this document also discusses, and presents in Table 2-1, public exposure standards and the assumed locations of the public, facility worker, and collocated worker for use in evaluation of accident consequences and normal radioactive material releases.

2.0 Exposure Standards for Facility and Collocated Workers

The four "To be derived" cells in DOE Table 1 have been completed by imposing a radiological exposure standard not to exceed 25 rem/event to the RPP-WTP facility workers or to collocated workers for either unlikely or extremely unlikely events.

The 25 rem/event exposure standard for both the facility and collocated workers for unlikely and extremely unlikely events corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2×10^{-2}. For unlikely events (defined in Table 2-1 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of only 2×10^{-4}, which is considerably less than the average accidental death risk for workers in some of the safest industries (i.e., retail and wholesale trade, manufacturing, and service [EPA 1991]).

Compliance with the 25 rem/event standard is established using qualitative methods supported, where necessary, by numerical analysis that may include the development of event trees and fault trees and/or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls are identified.

Use of qualitative methods is consistent with the American Institute of Chemical Engineers (AIChE) guidelines (AIChE 1992), U.S. Nuclear Regulatory Commission (NRC) guidance for the performance of integrated safety analysis for 10 *Code of Federal Regulations* (CFR) 70 special nuclear material licensees (NRC 1995a), as well as DOE-STD-3009 (DOE 1994) and DOE G 420.1-X (DOE 1995). Both DOE documents state the following:

> "Estimates of worker consequences for the purpose of a safety-significant SSC designation are not intended to require detailed analytical modeling. Considerations should be based on engineering judgement of possible effects and the potential added value of safety-significant SSC designation."

Because the primary purpose of the RPP-WTP Project facility and collocated worker exposure standards is to identify structures, systems, and components (SSC) required to protect these workers, the guidance cited above is both applicable and appropriate.

The principal approach for complying with the 25 rem/event worker exposure standard is the PHA. The PHA is a systematic, team-based review of the plant and treatment processes. The PHA identifies hazards and operability problems to a level of detail commensurate with the design detail available. Further hazard evaluation takes place in parallel with design development to ensure that safety continues to be built into the design process.

Having generated the list of hazards and hazardous situations, this list is subject to a further systematic team-based review where a binning process takes place. The binning process assigns postulated events to a certain hazard category and is essentially risk-based with categories of hazard defined according to a frequency/consequence matrix.

The 25 rem/event standard for unlikely or extremely unlikely events applies to events with frequencies less than 10^{-2}/yr. For those frequencies, the PHA process assigns serious and major hazardous situations as undesirable, acceptable with controls, or acceptable. For a hazardous situation to be "acceptable", its consequences must be less than 25 rem. Where there is uncertainty as to where an event should be binned (i.e., assigning a hazard category), it is binned into a higher category to ensure that the accident analysis remains conservative.

The DOE-RU has provided a guidance document (DOE-RL 1997) to be used for review of the Radiation Exposure Standard for Workers Under Accident Conditions. This guidance document includes the worker accident risk goal and the accident risk goal of DOE/RL-96-0006.

The worker accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to workers in the vicinity of the Contractor's facility, of fatality from radiological exposure that might result from an accident should not be a significant contributor to the overall occupational risk of fatality to workers".

DOE/RL-97-09 (DOE-RL 1997) describes approaches that can be taken to meet this goal. The simplest approach notes that the goal can be met when (a) a worker dose standard that does not exceed 100 rem is used for extremely unlikely events (10^{-4} to 10^{-6} probability range), and (b) a worker dose standard that does not exceed 10 rem is used for unlikely events (10^{-2} to 10^{-4} probability range). For the latter probability range, the 10-rem standard relies on the assumption that the probability of accidents is evenly distributed across the probability range.

Based on experience with similar plants, it is considered unlikely that the even distribution assumption will represent the actual situation for RPP-WTP. Furthermore, experience indicates that there will be relatively few accidents falling into this range, and that they will be distributed toward the low probability end of the range. Consequently, a value higher than 10 rem can be used for the worker accident standard for unlikely events.

As can be seen in Table 2-1, a value of 25 rem/event is selected as the worker accident standard for both unlikely and extremely unlikely events. Because this is over 10 rem for the 10^{-2} to 10^{-4} probability range, satisfaction of the worker accident risk goal needs to be demonstrated.

For the RPP-WTP, this goal is satisfied by calculating the risk of facility operation to the workers. This is a best estimate analysis based on realistic input and modeling assumptions. In performing this analysis, all structures, systems, and components capable of preventing or mitigating the event are considered. Estimates of system and component unavailabilities and unreliabilities consider failure to start and failure to run as well as maintenance-caused unavailabilities. Accident prevention and mitigation features are added to the design as necessary to satisfy the worker accident risk goal. Note 2 of Table 2-1 explicitly commits the RPP-WTP contractor to this risk evaluation process.

The accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to an average individual in the vicinity of the Contractor's facility, of prompt fatalities that might result from an accident should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed." The DOE guidance document states that a radiation exposure standard of 100 rem/event would satisfy the accident risk goal. Because the RPP-WTP standard is 25 rem/event, the guidance document is satisfied.

In each of the four cells addressing accident exposure standards for workers and collocated workers in the unlikely and extremely unlikely events ranges, an ALARA accident limit is not specified. However, Note 3 of Table 2-1 states:

> "In addition to meeting the listed dose standards for accidents, the approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below standards to account for uncertainties in the analysis, and to provide for sufficient design margin and operational flexibility."

This approach provides an adequate level of safety. The following paragraphs should also be noted in support of this conclusion.

The accident analyses will show compliance with exposure standards for accidents. In addition, a defense-in-depth approach provides multiple levels of protection that ensure worker exposures from accidents will be significantly lower than calculated. This is a proven approach, considered to be effective at minimizing exposures to workers.

The approach to accident mitigation (as described in Note 3 of Table 2-1) is to examine accident consequences to ensure that calculated exposures are far enough below standards to account for uncertainties in the analysis and to provide sufficient design margin and operational flexibility. This approach is employed for all accidents (including both public and workers at all accident frequency levels) that can challenge the exposure standards, ensuring that accident exposures would be well below standards.

3.0 Development of the BNI Approach to Compliance with Table 1 of DOE/RL-96-0006

The overall approach to complying with DOE Table 1 is presented in this document. This approach takes the form of Table 2-1. The "To be derived" cells have been completed as discussed. The remaining cells of Table 2-1 are either identical or conservative with respect to DOE Table 1. The following sections discuss differences between DOE Table 1 and Table 2-1.

DOE Table 1 footnotes are not shown in Table 2-1. Section 2.1 of DOE/RL-96-0006 states that the footnotes refer only to the origin of the specific standards and, as such, are not considered contractual requirements unless included elsewhere in the contract.

3.1 Estimated Frequency of Occurrence

The second column of DOE Table 1, "Estimated Probability of Occurrence (P) (yr^{-1})," has been titled in Table 2-1, "Estimated Frequency of Occurrence (f) (yr^{-1})". In addition, the estimated frequency of occurrence for normal events of DOE Table 1 is redefined in Table 2-1 as any normal event regardless of frequency (nominally taken to be a frequency > 0.1/yr). The estimated frequency of anticipated events in DOE Table 1 is redefined as events with an annual frequency of occurrence of $10^{-2} < f\ 10^{-1}$.

With these changes, events routinely performed (e.g., melter replacement) are considered normal events rather than accidents, irrespective of frequency of occurrence. As normal events, the radiological assessment is subject to the more restrictive "per year" exposure standards rather than "per event" exposure standards. Consequently, these changes are conservative in comparison to DOE Table 1.

3.2 Normal Events/Public and Workers Exposure Standards

Clarifying descriptions have been included in the Normal Events/Public cell of Table 2-1 explaining that the second 100 mrem/yr standard applies to a member of the public entering the controlled area and the 25 mrem/yr standard is the public primary exposure standard for radioactive waste. The removal of DOE Table 1 footnotes (as noted above) necessitated the addition of these clarifying notes.

For the Normal Events/Worker and Normal Events/Collocated Worker cells of Table 2-1, the DOE Table 1 standard of 1.0 rem/yr ALARA design limit is replaced by a standard of 1.0 rem/yr ALARA design objective per 10 CFR 835, Section 1002(b). The corresponding worker standards for normal events in DOE Table 1 are tied to the ALARA design objectives of 10 CFR 835.1002(b) by the footnotes to DOE Table 1.

BNI has committed to full compliance with 10 CFR 835 in the SRD, and the other sections of 10 CFR 835.1002 provide adequate requirements to ensure routine worker exposures will be ALARA. In addition, a footnote, Note 1, is included in Table 2-1. This note states the following:

> "In addition to meeting the listed design objective of 10 CFR 835.1002(b), the inhalation of radioactive material by workers and collocated workers under normal conditions is kept ALARA through the control of airborne radioactivity as described in 10 CFR 835.1002(c)."

3.3 Anticipated Events/Worker and Collocated Worker Exposure Standards

References to as low as reasonably achievable (ALARA) standards have been removed for the Anticipated Events/Worker and Collocated Worker cells of Table 2-1. The ALARA design objective of 10 CFR 835, "Occupational Radiation Protection", is applied to normal events as shown in Table 2-1. However, with the redefinition in Table 2-1 of anticipated events as those events with an annual frequency of occurrence of $10^{-2} < f \leq 10^{-1}$, the ALARA objective no longer applies because anticipated events are not part of normal operation.

This change complies fully with Section 3.2, "Radiation Protection Objective", of DOE/RL-96-0006, which states the following:

> "Ensure that during normal operation radiation exposure within the facility and radiation exposure and environmental impact due to any release of radioactive material from the facility is kept as low as is reasonably achievable (ALARA) and within prescribed limits, and ensure mitigation of the extent of radiation exposure and environmental impact due to accidents."

This aspect of Table 2-1 also represents compliance with contractual requirements because footnote 3 of DOE Table 1 references 10 CFR 835.1002(b). This section, and 10 CFR 835.202 which it references, establishes design requirements for occupational exposures other than planned special exposures and emergency exposures. Administrative limits for planned special exposures and emergency exposures are addressed in 10 CFR 835.204 and 10 CFR 835.1302 and are complied with by the RPP-WTP.

Finally, to provide an adequate level of safety and to ensure that cost-effective safeguards affecting anticipated events are evaluated (and incorporated as appropriate) whenever the final calculated event consequence to a worker or collocated worker is 1 rem or more, the approach specifies a 1.0-rem/event design action threshold standard. In addition, a note is included in Table 2-1 to explain the application of the standard. This note (Note 4 to Table 2-1) states:

> "When a calculated accident exposure exceeds this threshold, then appropriate actions are taken. These include carrying out a less bounding (i.e., more realistic) evaluation to show that the accident consequences will be below the threshold or evaluating additional safeguards for cost-effectiveness and/or feasibility. This threshold is not a limit; it does not require the implementation of additional preventative or mitigative features if they are not both cost-effective and feasible."

3.4 Extremely Unlikely Events/Public Exposure Standard

A standard is included in the Extremely Unlikely Events/Public cell of Table 2-1 stating that a public exposure standard target value of 5 rem/event is applied to extremely unlikely events. This target value is based on the following:

- The philosophy is that the public should be protected by a lower exposure standard than a worker. This philosophy recognizes the fact that the worker has agreed to work on the Hanford Site and has received training for avoiding hazards and dealing with hazardous situations.
- A goal to facilitate transition to the NRC as the regulatory agency with jurisdiction over nuclear safety for DOE facilities. With the exception of a 25 rem/event guideline value of 10 CFR 100 for the establishment of the exclusion area and low population zone for commercial power reactors, the NRC has not established a public exposure standard that exceeds 5 rem/event. A public exposure standard of 5 rem/event is also included in proposed rulemaking for 10 CFR 70 (NRC 1995b), which further supports the Table 2-1 value.
- With the same 5 rem/event public exposure standard for both unlikely and extremely unlikely events, there is no need to bin accidents in one of these two event frequency categories for the purpose of establishing protection of public safety.

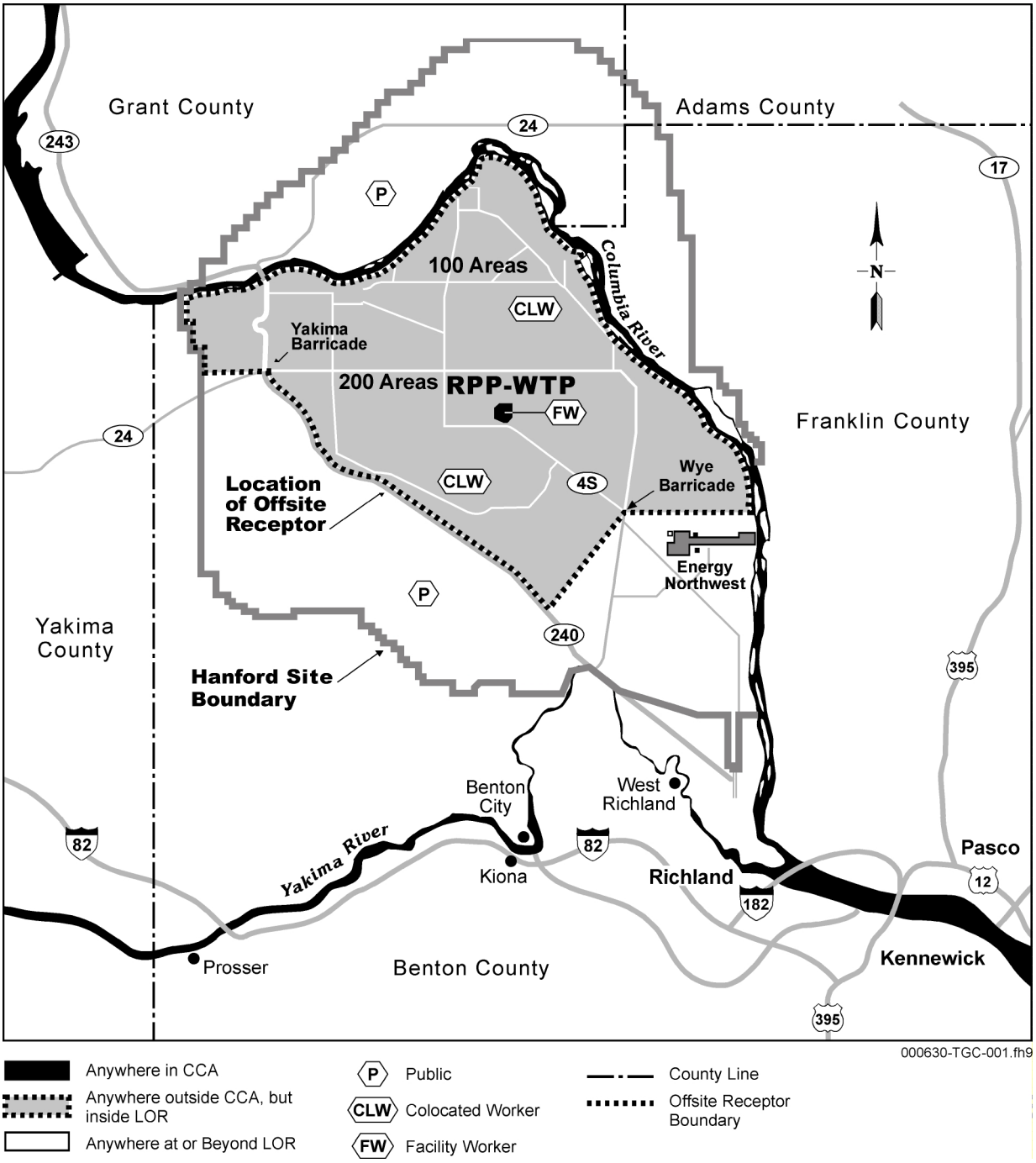
3.5 Location of Receptors

In Table 2-1, a new last row has been added to clarify in DOE Table 1 of DOE/RL-96-0006 the assumed location for the facility worker, the collocated worker, and the public, for the purpose of establishing compliance with the radiological standards of DOE Table 1. The bases for the receptor locations included in this row are provided below.

3.5.1 Facility Worker

The facility worker is located at the most limiting location within the RPP-WTP contractor-controlled area as defined in DOE/RL-96-0006, as shown in Figure D-1.

Figure D-1. Location of Facility and Collocated Workers.



Section 6.0, "Glossary", of DOE/RL-96-0006 defines the controlled area as the following:

> "The physical area enclosing the facility by a common perimeter (security fence). Access to this area can be controlled by the Contractor. The controlled area may include identified restricted areas."

The controlled area for RPP-WTP used to define the location of the facility worker, is that land within the RPP-WTP security fence.

3.5.2 Collocated Worker

Section 6.0, "Glossary", of DOE/RL-96-0006 defines the collocated worker as the following:

> "An individual within the Hanford Site, beyond the Contractor-controlled area, performing work for or in conjunction with DOE or utilizing other Hanford Site facilities."

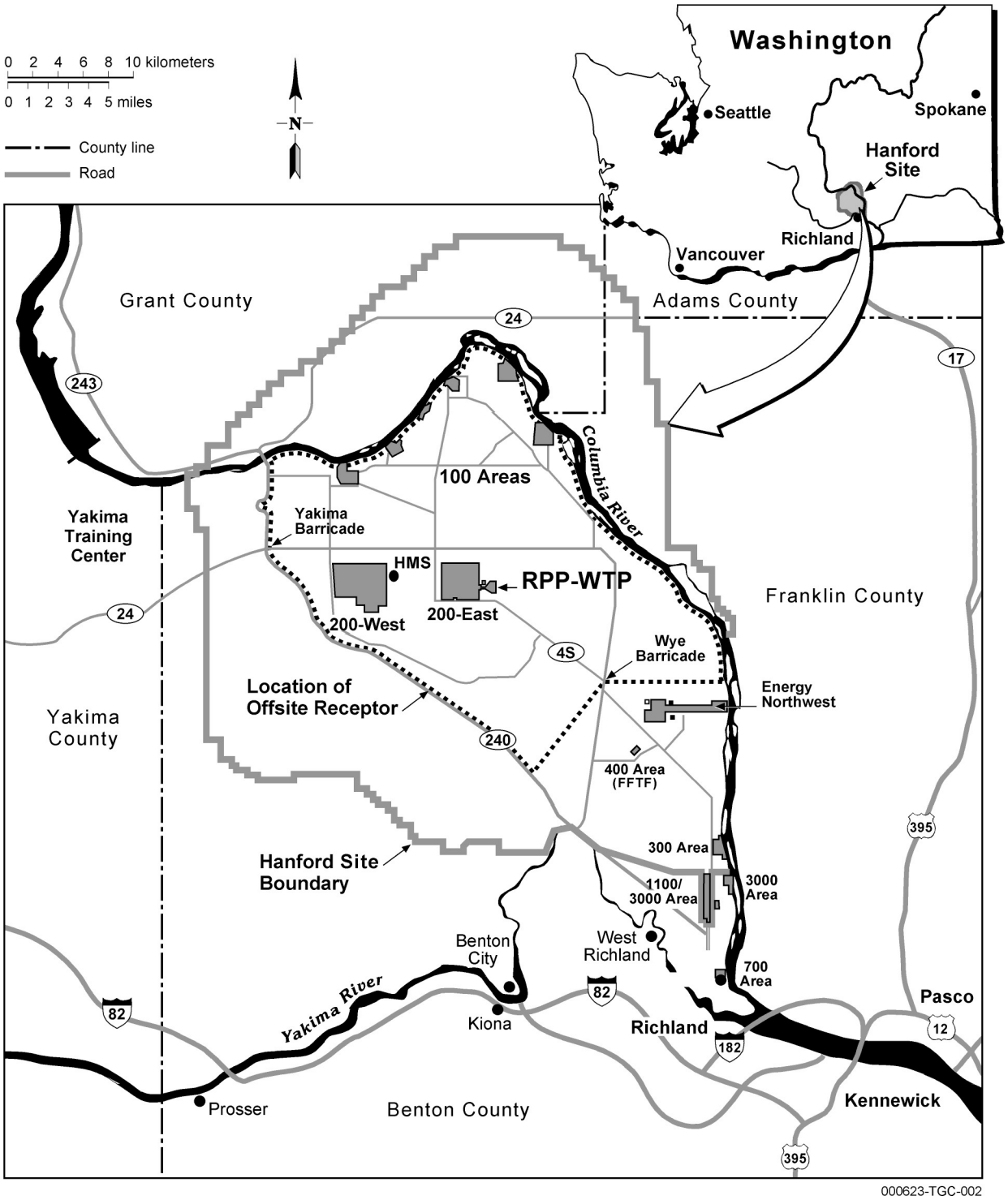
For evaluation of the RPP-WTP design to the exposure standards of DOE Table 1, the location of the collocated worker is either at the controlled area boundary or beyond that boundary if such a location results in higher exposure. For a ground-level release, the location of the collocated worker is considered no closer than 100 m from the release point.

3.5.3 Public

The location of the public (i.e., the offsite receptor) for the purpose of establishing compliance with the last column of DOE Table 1 of DOE/RL-96-0006, is established at the most limiting exposure location along the near bank of the Columbia River, Highway 240, and a southern boundary as shown in Figure D-2.

This area includes land for which it is reasonable to assume DOE will retain the right to control activities and limit access under accident conditions for the operating life of the RPP-WTP. Specifying the near river bank excludes the Columbia River for which DOE does not control activities (DOE-RL 1995). Specifying Highway 240 excludes the Arid Lands Ecology Reserve of which DOE might relinquish control during the operating life of the RPP-WTP. The southern boundary serves to exclude Energy Northwest's Columbia Generating Station, a commercial nuclear power plant (whose workers should be considered members of the public), and the Hanford Site 300, 400, and 1100 Areas. The 400 Area includes the Fast-Flux Test Facility.

Figure D-2. Boundary for Location of Offsite Receptor for the Purpose of Implementing DOE/RL-96-0006, Rev. 0, Table 1, Public Exposure Standard.



In footnotes 10 and 12, DOE Table 1 of DOE/RL-96-0006 makes reference to 10 CFR 72, "Licensing Requirements for the Independent Spent Fuel (ISFSI) and High Level Radioactive Waste," and 10 CFR 100, "Reactor Site Criteria," to relate to the public exposure standards for unlikely and extremely unlikely events. While the siting requirements and guidance of Parts 72 and 100 are not applicable to the RPP-WTP, the requirements for establishing the location of the offsite receptor in these two cited regulations are useful for locating the offsite receptor for a waste processing facility such as RPP-WTP. Section 72.106, "Controlled Area Boundary of an ISFSI or Monitored Retrievable Storage (MRS)", includes the following statements relative to the boundary to be assumed for the evaluation of radiological exposure to the public:

> "The minimum distance from the spent fuel or high-level radioactive waste handling and storage facilities to the nearest boundary of the controlled area shall be at least 100 meters."
>
> "The controlled area may be traversed by a highway, railroad or waterway, so long as appropriate and effective arrangements are made to control traffic and to protect public health and safety."

Title 10 CFR 100 establishes a guideline value of 25 rem for 2 hr at the exclusion area boundary. For the exclusion area, 10 CFR 100.3, "Definitions", states the following:

> "(a) *Exclusion area* means that area surrounding the reactor, in which the reactor licensee has the authority to determine all activities including exclusion or removal of personnel and property from the area. This area may be traversed by a highway, railroad, or waterway, provided these are not so close to the facility as to interfere with normal operations of the facility and provided appropriate and effective arrangements are made to control traffic on the highway, railroad, or waterway, in case of emergency, to protect the public health and safety. Residence within the exclusion area shall normally be prohibited. In any event, residents shall be subject to ready removal in case of necessity. Activities unrelated to operation of the reactor may be permitted in an exclusion area under appropriate limitations, provided that no significant hazards to the public health and safety will result."

As can be seen from the above excerpts, the assumed location for the offsite receptor for RPP-WTP is consistent with 10 CFR 72 and 10 CFR 100. In addition, the proposed southern boundary takes advantage of the road junction at the Wye barricade (Figure F-1) for control of access to the site during accident conditions.

4.0 References

10 CFR 70, "Domestic Licensing of Special Nuclear Material", *Code of Federal Regulations*, as amended

10 CFR 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-Level Radioactive Waste", *Code of Federal Regulations*, as amended

10 CFR 100, "Reactor Site Criteria", *Code of Federal Regulations*, as amended

10 CFR 835, "Subpart C - Standards for Internal and External Exposure", *Code of Federal Regulations*, as amended

AIChE, 1992, *Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York

DOE 1994, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, DOE-STD-3009-94, U.S. Department of Energy, Washington, D.C.

DOE 1995, *Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria*, DOE G 420.1-X, Revision G, U.S. Department of Energy, Washington, D.C.

DOE-RL 1995, *Clarification of Hanford Site Boundaries for Current and Future Use in Safety Analysis*, letter Walter B. Scott, DOE-RL to Contractors, dated September 26, 1995, U.S. Department of Energy, Richland Operations Office, Richland, Washington

DOE-RL 1996, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 0, U.S. Department of Energy, Richland Operations Office, Richland Washington

DOE-RL 1997, *Guidance for Review of TWRS Privatization Contractor Radiation Exposure Standards for Workers*, DOE/RL-97-09, U.S. Department of Energy, Richland Operations Office, Richland Washington

EPA 1991, *Manual of Protective Action Guides and Protective Actions for Nuclear Incidents*, U.S. Environmental Protection Agency, Washington, D.C.

NCRP 1963, *Maximum Permissible Body Burdens and Maximum Permissible Concentrations of Radionuclides in Air and in Water for Occupational Exposure*, Handbook 69, Addendum 1, National Bureau of Standards, Washington, D.C.

NRC 1995a, *Integrated Safety Analysis Guidance Document*, NUREG-1513, Draft, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1995b, *Preliminary Working Draft of Revision of 10 CFR 70 Updated*, 4/05/95, provided at the NRC public meeting of May 2, 1995, U.S. Nuclear Regulatory Commission, Washington, D.C.

Appendix E

Reliability, Availability, Maintainability, and Inspectability (RAMI)

To ensure that the facility meets operational requirements, it is necessary to address issues associated with reliability, availability, maintainability, and inspectability.

Reliability is used as a measure of the ability of an item or system to complete a task, and it is normally expressed as a probability of failure. Reliability is designed in through the use of appropriate design techniques and control of the mode of operation and the environment. Design techniques to be used vary because they are dependent on the specific item or system and the task to be performed. Their purpose is to optimize reliability by the following:

1) Use of proven materials and components
2) Design simplicity
3) Testability
4) Control of manufacturing standards
5) Control of operational mode (e.g., prevention of misuse and overloads)
6) Control of environment (e.g., protection against corrosion and vibration)

Consistent with the RPP-WTP process for tailoring hazard controls using the potential radiological and chemical consequences of individual events, reliability is assigned to SSCs based upon the importance of the SSC to the prevention or mitigation of accidents. The significance of accident prevention and mitigation is determined by the severity of the accident to workers or the public. To implement this tailoring in a clear, consistent, and defensible manner, an Implementing Standard for Safety Standards and Requirements Identification was developed. This Implementing Standard includes a Severity Level ranking system which provides the hazard assessment and control teams with a defined way to categorize the potential severity of those events that can result in radiological or hazardous exposure to the workers or the public. The Implementing Standard provides the means by which the hazard assessment and control teams establish target reliabilities for SSCs.

Availability is a measure of the degree to which an item or system is in an operable condition. It is expressed quantitatively as the ratio of the mean time between failures to the sum of the mean time between failures and the mean time to repair. System availability is calculated to determine the potential for downtime. In this way, systems are identified that contribute to decreased availability. Required availability is achieved by specifying additional systems or increasing reliability of existing systems.

Maintainability is a measure of the ability to restore a failed item or system to an operable condition in a specified time. Maintainability is designed into the facility and processes through use of appropriate design techniques, (e.g., the use of specially designed, remotely removable, and replaceable pumps and valves in process systems, and the placement of active pumps or valves within shielded accessible areas equipped with appropriate decontamination facilities that allow hands-on maintenance activities) and logistic support (e.g., scheduling and procedures). Benefits of these design techniques are that they simplify maintenance operations in high radiation areas and remove high maintenance equipment from high radiation areas. Testability of Safety Design Class systems and components is facilitated by such features as redundancy that allow for a system or component to be removed from service for maintenance or testing without loss of safety protection.

Inspectability is the measure of the ease with which items or systems can be inspected for preventative maintenance or assessment of condition. Inspectability is used to monitor facility items in order to maintain their reliability. Inspectability of facility items can be designed in by the use of shielded access areas (as above, to reduce radiation exposure) for active equipment or the provision of monitoring equipment (e.g., material coupons for determining vessel corrosion rates, and in-cell cameras).

During the design phase, the RPP-WTP facility and processes are evaluated for reliability, availability, maintainability, and inspectability. A number of validated modeling techniques (computer codes, mathematical modeling, failure modes, and effects analysis) for determining reliability and availability of the facility and processes are used. These are used to identify those facility and process areas that are sensitive with respect to influencing overall facility and process performance. Optimum reliability is established by the use of appropriate standards and quality control. The determination of maintenance and inspection needs is based on facility and process reliability requirements. It is a mixture of process optimization, provision of appropriate design features to aid preventative and scheduled maintenance and inspection, and the development of maintenance and inspection programs (administrative and procedural controls) whose objectives among other things, are to facilitate these activities. Reliability targets are assigned to SSCs only when a quantitative value has been credited for the reliability of an SSC in safety analysis.

Appendix F

Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning

CONTENTS

Section **Page**

1.0 Introduction F-1
2.0 Plan Preparation F-1
3.0 Summary F-2
4.0 Definitions F-2

1.0 Introduction

All elements of the RPP-WTP safety approach are applied to the deactivation phase of the project. In addition, the RPP-WTP will incorporate design provisions to facilitate deactivation and final decommissioning as described in the implementing standard DOE G 441.1-2, *Occupational ALARA Program Guide*, for SRD Criterion 8.0 - 2. These provisions will reduce radiation exposure to Hanford Site personnel and the public during and following deactivation and decommissioning activities and minimize the quantity of radioactive waste generated during deactivation. The purpose of this standard is to define the attributes that must be addressed during the preparation of the deactivation plan to protect both the Hanford Site personnel and the public both during and after the deactivation stage of the project.

2.0 Plan Preparation

A deactivation plan will be prepared prior to construction of the RPP-WTP. The deactivation plan will provide details on how the following activities will be accomplished to achieve a deactivated status for the facility.

1) Verification of the completion of the facility deactivation end point. The term facility deactivation end point refers to the set of conditions that comprise the completion of facility deactivation i.e., radiological, structural, equipment, and documentation. These general end points will be defined in the deactivation plan and a requirement made to determine specific end points. When these end point criteria are met the facility will be in a safe state that can be economically monitored and maintained until final decommissioning.
2) Documentation of the regulatory status, conditions, and inventories of remaining radioactive and hazardous materials and health and safety requirements. After facility construction but before deactivation commences, the deactivation plan will require a hazard evaluation for radiological, nuclear, and process safety be carried out. Safety standards and requirements will be identified to implement the controls to protect against the facility hazards.
3) Identification of the facilities, structures, support systems, and surveillance systems to provide for confinement and monitoring of the remaining contamination, radiation, and other potential hazards. After facility construction but before deactivation commences, the plan will be expanded to describe the activities required to maintain the operability of critical equipment and to maintain the structural integrity of the deactivated facility. It will identify modification requirements to systems for the above purposes.
4) Posting and securing of the facility. After facility construction but before deactivation commences, the plan will be expanded to identify the radiological controls required for the deactivated facility, which will include posting of radiological areas. The need for other safety postings will also be identified.

5) Removal of packaged special nuclear materials and other packaged radiological and chemical materials.
6) Confirmation that security systems and procedures are adequate and in place to prevent unauthorized entry.
7) Waste minimization during the deactivation process.

3.0 Summary

The above requirements for the deactivation plan in combination with measures taken at the design stage of the project will protect the Hanford Site personnel and the public both during and following the deactivation activities.

4.0 Definitions

Deactivation - Placing the facility in stable and known conditions, identifying hazards, eliminating or mitigating hazards, and transferring programmatic and financial responsibilities from the operating program to the disposition program. Surveillance and maintenance continues to assure public, environment, and worker safety. The facility is in a safe storage mode, with ongoing, low levels of surveillance and maintenance. The general intent is that the facility be unoccupied and locked except for periodic inspections. Radioactive and hazardous materials may remain in the facility and are subject to ongoing regulatory oversight. (DOE/EM-0318, *Facility Deactivation Guide -- Methods and Practices Handbook*, December 1996)

Decommissioning - The process of removing a facility from operation, followed by decontamination, entombment, dismantlement, or conversion to another use. (DOE G 430.1-1A, *Life Cycle Asset Management*)

Decontamination - The reduction or removal of contaminating radioactive material from a structure, area, object or person. Decontamination may be accomplished by (1) treating the surface to remove or decrease the contamination, (2) letting the material stand so that the radioactivity is decreased as a result of natural decay, and (3) covering the contamination to shield or attenuate the radiation emitted. (Health Physics and Radiation Health Handbook, Revised Edition, Bernard Shleien, 1992)

End Point - Specifying and achieving end points is a systematic, engineering way of proceeding from an existing condition to a stated desired final set of conditions in which the facility is safe and can be economically monitored and maintained. (DOE/EM-0318, *Facility Deactivation Guide - Methods and Practices Handbook*, December 1996)

Appendix G

Ad Hoc Implementing Standard for Safety Analysis Reports

CONTENTS

1.0 Introduction G-1
2.0 Definitions G-1
3.0 Process G-1
    3.1 Safety Analysis Report Preparation G-1
4.0 References G-25

1.0 Introduction

The purpose of this Implementing Standard is to define the format and content for RPP-WTP safety analysis reports (SARs).

Section 2.0 provides the definitions important to this Implementing Standard. Section 3.0 defines the process for development, review, and approval.

2.0 Definitions

For the definitions of the following terms, see the reference provided.

Safety Analysis Report (SAR) (DOE/RL-96-0006 [DOE-RL 1998b])

3.0 Process

3.1 Safety Analysis Report Preparation

The River Protection Project Waste Treatment Plant (RPP-WTP) SARs document the safety analyses for the facility to demonstrate that it can be safety operated, maintained, and shut down.

The SARs shall be prepared in accordance with the requirements of:

1) DOE/RL-96-0003, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors* (DOE-RL 1998a), Sections 4.3.2 and 4.3.3, both titled "Contractor Input"
2) Contract Table S7-1, "Radiological, Nuclear, and Process Safety Deliverables"
3) *Safety Requirements Document Volume II* (SRD) (BNI 2001), Safety Criterion 9.1-2

The content of the Preliminary Safety Analysis Report (PSAR) and the Final Safety Analysis Report (FSAR) are developed using the guidance provided in the Nuclear Regulatory Commission's 1995 draft revision to Regulatory Guide 3.52, *Standard Format and Content for Heatlh and Safety Sections of License Applications for Fuel Cycle Facilities* (NRC 1995). The content of the SARs is tailored to the nature of the RPP-WTP relative to the hazards and hazardous situations identified by the process hazards analysis. Planned deviations from the content guidance of draft Regulatory Guide 3.52 are identified in Table G-1.

The Table of Contents for the safety analysis reports follows Table G-1. The safety analysis report will not be submitted to the regulator until all major safety issues have been resolved and other safety issues have been scheduled for completion. The FSAR should identify significant changes made in the facility design and plans for operation from what was presented in the PSAR. The FSAR, in addition to including facility and process drawings, should also include fabrication and construction specifications important to the safety analysis of the facility.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
1.3 Site Description	Regulatory Guide (RG 3.52) suggests that Section 1.3 summarize information used in preparing the Environmental Report. Specific information is referenced, but not duplicated in the safety analysis report (SAR).	The Environmental Report provides this information.
1.3.2 Demography and Land Use	The population distribution as a function of distance and direction is not to be provided. The distances to nearby population centers are provided.	There are no residences on the Hanford Site and the nearby population is low.
3.3 Quality Assurance	Section 3.3.4, "Quality Assurance Program Description" addresses the 10 criteria of 10 CFR 830 Subpart A, "Quality Assurance Requirements" in lieu of the 18 criteria listed in RG 3.52.	By contract compliance to the 10 CFR 800 series of nuclear safety requirements is required. This includes compliance to 10 CFR 830 Subpart A, "Quality Assurance Requirements". The differences in the criteria to be addressed are not significant because the quality assurance programs are based on consensus standards.
3.5 Human Factors	RG 3.52 states that a formal human factors program is not required if the facility has no requirement for safety-class actions. Human factors are considered in the Preliminary Safety Analysis Report (PSAR) independent of whether or not human actions are required for protection of the public or workers.	The requirements of DOE/RL-96-0006 (DOE-RL 1998a), Section 4.2.6, "Human Factors", extend beyond consideration of human factors as related to actions taken to protect the public. Final Safety Analysis Report (FSAR) Section 3.5 documents how compliance to contract Section 4.2.6 is achieved.
3.10 Testing Program and Preoperational Safety Review	This section is added to address the initial and commissioning testing programs.	Addition of this section facilitates documentation of compliance to DOE/RL-96-0006 (DOE-RL 1998b), Section 4.2.8, "Pre-Operational Testing", and Section 5.2.6, "Pre-Startup Safety Review", and DOE/RL-96-0003 (DOE-RL 1998a), Section 4.3.2, "Contractor Input", item 13.
3.11 Operational Practices	This section is to added to address such conduct of operations considerations as shift routine and turnover, control area activities, communications, control of on-shift training, control of equipment and system status, lockout and tagout, independent verification of equipment status, logkeeping, and operational aids postings.	These items are discussed to address what is normally considered conduct of operations.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
4.7 Results of the Integrated Safety Assessment	The results for unmitigated accidents are compared to the radiological standards discussed in Integrated Safety Management Plan (ISMP) Section 1.2, "Detailed Description of the Safety Approach" rather than to 10 CFR 20, "Standards for Protection Against Radiation". A full assessment of the hazardous situations that might present themselves during facility operation is provided. This includes estimates of radiological and chemical releases for this range of events. Additional details are provided on the methodology used for consequence analysis, bounding conditions, input assumptions, and accident sequences.	The standards provided in RG 3.52 were derived from 10 CFR 20, "Standards for Protection Against Radiation", which is applicable to normal operation. The nature of the accidents for the RPP-WTP requires more discussion of consequence analysis than that required of fuel fabrication facilities.
4.8 Controls for Prevention and Mitigation of Accidents	This section identifies the specific safeguards selected for protection of the facility workers, as well as safeguards selected for protection of the public and collocated workers.	The nature of the accidents for the RPP-WTP requires more discussion of consequence analysis than that required for fuel fabrication facilities.
5.0 Radiation Safety	Chapter 5.0 provides the upper-level statutory standards and program policies that ensure the radiological safety of employees, visitors, and onsite members of the public. Deviations from RG 3.52 are as follows: 1) As an U.S. Nuclear Regulatory Commission (NRC) document, RG 3.52 references and specifies applicable portions of 10 CFR 20. Because 10 CFR 835 is the radiation safety regulation for the RPP-WTP, the focus of this section is on 10 CFR 835. 2) The implementation-level standards and guidance documents referenced in RG 3.52 is being incorporated into the Radiation Protection Plan (RPP).	Compliance with 10 CFR 835 is a requirement of the contract. The RPP required by 10 CFR 835 is required to include some of the information required of RG 3.52. There is no need to present this information in two documents.
5.1 As Low As Reasonably Achievable (ALARA) Policy and Program	RG 3.52 states that Regulatory Guide 8.10, Revision 1R (*Operating Philosophy for Maintaining Occupational Radiation Exposures As Low As Reasonably Achievable)* should be used in the development of the ALARA program. DOE guidance such as DOE G 441.1-2, *Occupational ALARA Program Guide* will also be used to develop the RPP-WTP ALARA program for normal operation.	DOE practices have proven to be successful for facilities similar to the RPP-WTP.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
5.3 Radiological Safety Standards	Section 5.3 is added to provide the radiation standards by which the program operates. The standards specifically identify regulatory exposure standards, administrative exposure control levels, and other key standards of the radiation protection program.	The contract requires compliance to the 10 CFR 800 series of nuclear safety requirements. This includes compliance to 10 CFR 835, "Occupational Radiation Protection". Section 5.3 documents the compliance to the exposure standards of those regulations that have been promulgated.
5.8 External Exposure (renumbered 5.9 from RG 3.52)	By RG 3.52, the applicant is expected to participated in the National Voluntary Laboratory Accreditation Program (NVLAP) external dosimetry. Section 5.8 allows for participation in either the NVLAP or U.S. Department of Energy (DOE) Laboratory Accreditation Program (DOELAP) accreditation programs.	The option of participating in either the NVLAP or the DOELAP provides maximum flexibility and equivalent dosimetry program quality
5.14 Radioactive Waste Management	RG 3.52 does not require a discussion of waste management systems.	Section 5.14 is added to the SARs as the Process Hazards Analysis (PHA) completed for the RPP-WTP have identified hazards and hazardous situations with the waste management features of the facility. It is a requirement of DOE/RL-96-0003 (DOE-RL 1998a), Section 4.1.2, "Contractor Input", that deliverables be tailored to the nature and level of hazards associated with its waste processing activities.
Appendix 5A Radiation Protection Program Outline	This appendix is added to address compliance to 10 CFR 835.	The contract requires compliance to the 10 CFR 800 series of nuclear safety requirements. This includes compliance to 10 CFR 835, "Occupational Radiation Protection".
Appendix 5B Environmental Radiation Protection Program Outline	This appendix is added to address compliance to the requirements of the Environmental Protection Agency (EPA) and Washington State laws and regulations.	The contract requires submittal of an outline for the environmental radiological protection plan.
Chapter 6.0 Nuclear Criticality Safety	The methodology for criticality analyses is provided in the SARs to the extent the need to perform criticality calculation is found to be appropriate. The RPP-WTP SARs provide fewer details and commitments compared to fuel fabrication facilities relative to: 1) Nuclear criticality safety organization (Section 6.2.1) 2) Criticality training (Section 6.2.5) 3) Specific maintenance and quality assurance provisions for criticality prevention (Sections 6.2.3 and 6.2.4) 4) Audits and inspection (Section 6.2.6)	RG 3.52 focuses heavily on accidental criticality which is a more significant concern for fuel fabrication facilities which have a much higher inventory and concentrations of fissile material than the RPP-WTP. See ISMP Section 3.8, "Criticality Safety", for additional information.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
7.4 "Hazardous Waste Management"	Section 7.4 of the RPP-WTP SARs address all chemical inventories that are identified by the PHA as representing a significant hazard.	By Section 4.2.2, "Contractor Input", of DOE/RL-96-0003 (DOE-RL 1998a), the Initial Safety Analysis Report (ISAR) is to address process safety as well as radiological and nuclear safety. The need to address all aspects of chemical safety is also a NRC requirement of RG 3.52, Section 7.4, and NUREG-1513, "Integrated Safety Analysis Guidance Document", (draft) (NRC 1994). The NUREG-1513 definition of "integrated" provided in Section 2.1, "Definition", makes reference to chemical safety. Specific guidance for chemical safety is provided in Section 2.6.2, "Process Safety Information", of the NUREG-1513.
10.0 Environmental Protection	This chapter references the Environmental Report	Protection of the environment is addressed in a separate document.
11.0 Deactivation and Decommissioning	This chapter addresses design and operational provisions considered to facilitate deactivation and decommissioning. It does not address the financial considerations for decommissioning.	The scope of the contract (DOE-ORP 2000) is limited to design support for deactivation.

1. Standard Format and Content for the Health and Safety Sections of License Applications for Fuel Cycle Facilities, Regulatory Guide 3.52, Revision 2, draft, U.S. Nuclear Regulatory Commission, Washington D.C. (NRC 1995).

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
1.1.1 Facility Description	A description of the facility design is provided in sufficient detail to demonstrate the facility design and construction requirements of the Safety Requirements Document (SRD). The details are also sufficient to support an understanding of the safety analysis provided in section 4.2, "Facility Description".	This section updates the general description of the facility design.
1.1.2 Process Description	This section describes the process design in sufficient detail to demonstrate the system and component design and fabrication requirements of the SRD are satisfied. Details on the process design sufficient to support an understanding of the safety analysis are provided in section 4.3, "Process Description".	This section updates the general description of the process design.
1.2 Institutional Information	This section provides the information required by RG 3.52, draft (NRC 1995a).	This section updates any changes in the institutional information provided in the PSAR.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
1.3 Site Description	A description of the site land use, meteorology, hydrology, geology, and seismology is provided.	This section address any existing or planned changes in land use from that provided in the PSAR. The FSAR provides any new meteorology, hydrology, geology, and seismology data made available. However, the level of detail provided for these subject areas is not significantly different between the two SARs. The FSAR summarizes data obtained during the Facility excavation that confirms the adequacy of the design. This includes the results of field and laboratory investigation of soil properties.
2.1 Organization and Administration	The Project organizational charts with a focus on the design and construction management organizations are provided. An organization chart for the operational phase is also presented. More definitive information on the roles, responsibilities, and interfaces for project management, engineering, construction management, inspections, procurement, quality assurance, records management, and nuclear safety functions is included. Section 2.1 also provides the criteria to determine minimum staffing requirements. A summary of procedures to be developed to implement the regulatory requirements addressed in this section is presented.	The section contains an update to the organizational structure of Project with a focus on operational and operational support organizations. This section also includes: 1 Title of each position that is important to public and worker safety and reporting relationship 2 Description defining qualifications, responsibilities, and authorities for each position related to safety 3 Organizational charts of the line organization and safety organization 4 Title of the individual delegated overall responsibility for the safety programs who has the authority to shut down operations if they appear to be unsafe, including independence of this authority from operational constraints 5 Lines of responsibility and authority for safety 6 Lines of communication and interfaces between organizations inside the facility 7 Availability of personnel within the safety organization to carry out the assigned function Specific information on procedure development and minimum staffing requirements is provided.
2.2 Safety Committees	Information on responsibilities, authorities, and proposed charters of safety committees, and oversight groups is provided.	This section updates information on safety committees, and oversight groups that are established following issuance of the PSAR and addresses any new safety committees that have been established.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.1 Configuration Management	This section contains specific information on: 1 Content and reference to procedures used to maintain effective configuration management of the RPP-WTP 2 Scope of identified systems, structures, and components (SSCs) and their relationship to the contents of Chapter 4.0, "Integrated Safety Analysis" 3 Description of the design information package contents to be provided to the safety analysts 4 Change control system specifics, including identification, technical and management reviews, documentation, and implementation 5 Specific physical configuration assessment, and periodic equipment performance monitoring 6 Design, installation, and testing of facility modifications 7 Revision of operating, test, calibration, surveillance, and maintenance procedures and drawings 8 Selection and control of replacement parts 9 Description of how the RPP-WTP design requirements and design basis were established and documented A summary of procedures developed to implement the regulatory requirements addressed in this section 3.1 is presented. This section also includes a draft of the unreviewed safety question process.	Specific information on the content of procedures and training developed is provided. The final unreviewed safety question process is provided.
3.2 Maintenance	A list of Safety Design Class and Safety Design Significant SSCs is provided. The maintenance implementation plan is described to such a level that maintenance philosophy and approach are evident.	The FSAR may modify the list of SSCs actions to be addressed based on safety analysis of the final design. Specific information on procedures and training developed to implement the requirements of section 3.2 is provided. In addition, the elements of the finalized maintenance implementation plan is described. Also discussed is the application of information obtained from demonstration testing and commissioning programs to the maintenance program (the latter by FSAR amendment after initial submittal).

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.3 Quality Assurance	Information related to the roles, responsibilities, and interfaces for project management, engineering, construction management, inspections, procurement, quality assurance, records management, and nuclear and process safety functions is provided. Included is the organizational structures of the quality assurance organization. The PSAR describes the quality assurance requirements of SSCs. Requirements for procedures to implement the regulatory requirements is presented.	For the FSAR, this section focuses on the quality assurance program for the operating RPP-WTP. Specific information on procedures and training developed to implement the requirements of section 3.3 is provided.
3.4 Training and Qualification	A description of the performance-based training program for operational and support personnel, including a detailed description of the training development process, is provided. The administrative process to be applied to training activities is described to a level such that the elements of the program and management's commitment to training is evident.	Details on the training and qualification program are provided. Also discussed is the application of information obtained from demonstration testing and commissioning programs (the latter by FSAR amendment after initial submittal).
3.5 Human Factors	This section documents the criteria by which human factors are considered in the facility design and operation.	This section states how human error in facility operations was taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions. Consideration given in the design to detecting and correcting or compensating for errors is discussed.
3.6 Audits and Assessments	Information on the performance of audits and assessments is incorporated into this section.	This section is focused on audits and assessments performed during RPP-WTP operation. Specific information on procedures and training developed to implement the requirements of this section is provided.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.7 Incident Investigation	This section includes the following: 1 Provisions for establishing investigating teams 2 Functions, responsibilities, and scope of authority of investigating teams 3 Qualifications of internal and/or external investigators on investigating teams 4 A description of the procedures to ensure prompt investigation of an incident 5 Policy directives that the investigative process and the investigating team be independent of line management and that participants be assured of no retribution from participating in investigations 6 The approach proposed to determine the root cause(s) of incidents to ensure that the process is reasonable, systematic, and structured 7 Methods to ensure that corrective actions to resolve findings from incident investigations are tracked to completion 8 Identification and application of lessons learned 9 Specific reporting criteria for incident reporting during the construction phase. A summary of procedures developed to implement the regulatory requirements addressed in section 3.7 is presented.	Specific information on procedures and training developed to implement the requirements is provided. Included are specific reporting criteria for incident reporting during the operations phase.
3.8 Records Management	This section contains the organization structure and a description of the records management system, including authorities, responsibilities, and qualifications of personnel managing Environmental, Safety, and Health (ES&H) records. A summary of procedures developed to implement the regulatory requirements contained in section 3.8 is presented.	Specific information on procedures and training developed to implement the requirements is provided.
3.9 Procedures	A description of the administrative controls to ensure that work is performed in accordance with established technical standards and using approved instructions and procedures is provided.	This section describes the detailed processes of selecting activities requiring operating, emergency, and support procedures; preparing procedures; verifying and validating procedures; and reviewing and approving procedures. In addition, the program to administratively control procedures and their use is described in detail.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.10 Testing Program and Preoperational Safety Review	This section describes the analysis used to identify and define pre-operational and commissioning tests and describes tests required to ensure compliance to safety specifications. The testing program and controls are described to a level such that the testing philosophy and approach are evident. The prestart safety review approach is described to a level such that the areas to be evaluated and the evaluation approach are evident.	This section may modify the list of required safety improvement program and commissioning tests based on safety analysis of the final design. In addition, the administrative and program controls applicable to the test program are described in full.
3.11 Operational Practices	A description is provided of operational practices influenced by design details (i.e., communications systems, operational hazards associated with systems and hardware, and control area arrangements).	A description is provided of the operational practices influenced by the final design. In addition, final descriptions are provided on controls and administration of operational practices.
4.0 Integrated Safety Analysis	The methodology for hazards identification and accident analyses is described. The accident consequence analyses include margins in assumptions, boundary conditions, modeling and comparisons to acceptance criteria, as appropriate, to account for uncertainties in the design and plans for operation. Section 4.7 addresses the relationship of these uncertainties to the need to provide sufficient information in the construction authorization package to allow for issuance of the construction authorization.	Assumption used the PSAR to account for uncertainties in the design and plans for operations are removed from the FSAR analysis to the extent that these uncertainties have been resolved.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.2 Facility Description	In addition to providing a general description of the facility, this section discusses the basic civil/structural criteria to be applied to the design. For those structures classified as Safety Design Class, this includes the following: 1 Design codes, standards, and specifications 2 Loading criteria and load combinations 3 Design and analysis methodology 4 Structural acceptance criteria 5 Criteria for identifying testing and in-service inspection requirements 6 Material specifications 7 Special construction features This section also discusses: 1 Assumed soil properties 2 Excavation, backfill, and recompaction criteria 3 Assumed bearing capacity of the soil and the safety factor applied to this capacity 4 Expected static and dynamic building total and differential settlements. Less detail is provided for Safety Design Significant structures. Section 4.2 gives specific attention to those structures classified in Section 4.8 as Safety Design Class. Structures located away from the buildings containing significant hazards and that have no relationship to nuclear or process safety are briefly described (e.g., structural design, and the contents and functions of the building) and identified on a plot plan.	The FSAR updates the facility description and basic civil/structural criteria provided in the PSAR. It follows with discussions of the results of the application of these criteria to specific features of the facility. Examples are as follows: 1 The confirmation of soil properties obtained during excavation 2 A table providing the building total and differential settlement data obtained 3 Derived soil damping values 4 The results of the soil/structure analysis 5 Developed floor response spectra and time histories 6 A list of moderate and high energy systems 7 A list of specific missile and jet impingement sources, targets, and barriers provided. Also provided are updated plan and section drawings for structures classified as Important-to-Safety. These drawings show the basic floor arrangements, location of major systems and equipment, and basic building dimensions. For those structures classified as Safety Design Class, the drawings also show key structural elements, such as panel and floor reinforcements, cell liners, leak chases, major equipment anchors, and the use of masonry walls.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.3 Process Description	The description of process systems includes process flow diagrams for the major systems with instrumentation, sample points, and control features noted to the extent they have been developed. Heat loads are provided for heat transfer systems important to the safety analysis. Design features and parameters important to Section 4.7, "Results of the Integrated Safety Assessment", are provided. This section contains the following additional detail for each system classified as Safety Design Class: 1 The specified safety function(s) with reference to PSAR Section 4.7 for the basis 2 The design basis to be applied in the development of the system design 3 Design margins to be applied 4 The criteria to be used for the development of material specifications 5 Criteria to be used to determine design limits (such as pressure and temperature) 6 Criteria to be used to identify the need for instrumentation to monitor process conditions and the design criteria for such instrumentation (e.g., application of the single-failure criterion, and testability). For many cases, the design criteria provided are those included in the SRD.	This section updates the PSAR description of process systems. Process and instrumentation diagrams are provided for major systems. In addition, for those systems classified as Safety Design Class, the FSAR describes how the design requirements provided in the PSAR are reflected in the final design. For each system classified as Safety Design Class, the following are provided: 1 The specified safety function(s) with reference to Section 4.7 for the basis 2 The design basis 3 The design safety margins provided by the final design 4 Important quantitative design parameters met by the system design with their basis (e.g., heating, ventilation, and air-conditioning flow, and what established the minimum and maximum flow limits) 5 Material specifications 6 Established design limits and their basis (e.g., maximum pressure and temperature limits and what established these limits) 7 Instrumentation provided with attributes, including redundancy, diversity, in situ testability, environmental qualification, failure mode on loss of power, and the surveillance requirements as defined in section 4.8, "Controls for Prevention and Mitigation of Accidents". The means by which the monitoring requirements established in section 4.8 are also to be discussed in the FSAR. Potential adverse system interactions between systems of various design classification are addressed.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.7 Results of the Integrated Safety Analysis (ISA)	In addition to providing the results of the Process Hazards Analysis (PHA) and accident analysis, this section discusses the uncertainties of the PHA and accident analysis and relates these uncertainties to the required content of the construction authorization package. Section 4.7 provides the basis for the conclusion that resolution of the uncertainties will not have a significant impact on the construction authorization request. This discussion includes the following: 1 Characterization of the specific technical information that must be obtained to demonstrate acceptable resolution of the uncertainties 2 An outline and schedule of the program to resolve uncertainties 3 A discussion of the design and/or operational alternatives to resolve the uncertainties Section 4.7 of the PSAR also describes the preliminary Fire Hazard Analysis (FHA) and the consequence of each design-basis fire scenario, including the consequences in the area of origin and adjacent areas.	This section documents the resolution of any uncertainties identified in the PSAR. The FSAR describes the final FHA and all resolved uncertainties previously included in the PSAR and additional fire protection measures and equipment design.
4.8 Controls for Prevention and Mitigation of Accidents	Draft Technical Safety Requirements are included.	Final Technical Safety Requirements are included.
5.0 Radiation Safety	This chapter identifies the radiological exposure standards by which the radiation safety program is developed and the facility is operated to ensure the radiological safety of the public and workers. This chapter identifies the radiation protection criteria to be implemented in the facility design.	This chapter reflects the final facility design developed to the radiation protection criteria. It also describes the facility organization and plans for the conduct of operations. This chapter includes detail on facility operation within the radiological protection program exposure standards and other radiological protection requirements.
6.0 Criticality	The methodology for criticality analyses is provided to the extent the need to perform criticality calculation is found to be appropriate. The analyses may include margins in assumptions, bounding conditions, modeling and comparisons to the acceptance criterion, as appropriate, to account for uncertainties in the design and plans for operation.	Assumptions used in the PSAR to account for uncertainties in the design and plans for operations are removed from the FSAR criticality analysis to the extent that these uncertainties have been resolved. The FSAR describes the remaining criticality controls appropriate for the RPP-WTP.
7.0 Chemical Safety	The chapter identifies the program standards by which the chemical safety program is developed and operated to protect the public and workers against chemical hazards and hazardous situations. This chapter identifies criteria to be used for the development of chemical safety controls.	The chapter reflects the final facility design and facility organization and the developed plans for conduct of operations as related to chemical safety. This section also identifies the specific chemical safety controls to be implemented for protection of the public and workers.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
8.0 Fire Safety	This chapter describes automatic and manual fire protection features and administrative controls of the fire safety program. Also described are features of the ventilation system, building layout, and emergency egress routes important to fire safety.	Administrative controls to be implemented for the fire safety program are described, including final responsibilities of response forces, and the pre-fire plan used by firefighting personnel to suppress fires safely and effectively.
9.0 Emergency Management	This chapter identifies the applicable requirements and criteria to which the RPP-WTP Emergency Management Program are developed. A general outline of the program is presented and the relationship to the Hanford Site and local emergency management programs is discussed. Information is presented to demonstrate that the RPP-WTP staff will be able to attain an acceptable state of emergency preparedness by the time the facility becomes operational.	The FSAR discusses and references the specific emergency plan and implementing documentation prepared for the RPP-WTP. Specific aspects of all elements of the emergency preparedness program are discussed. Information is presented demonstrating the developed emergency preparedness program is compliant with applicable requirements, regulations, criteria, and guidance, and capable of responding to any operational emergency at the facility.
10.0 Environmental Protection	This chapter references the RPP-WTP Environmental Report submitted in Part A.	This chapter references the RPP-WTP Environmental Report as a new or revised Environmental Report and is not required to support the operating authorization request.
11.0 Deactivation and Decommissioning	This chapter identifies design considerations given to facilitate deactivation and decommissioning. It also discusses in general terms the planning, safety analysis, and regulatory considerations to be given to deactivation.	The chapter describes the specific design features included to facilitate deactivation and decommissioning. The level of detail for planning, safety analysis, and regulatory considerations to be given to deactivation is about the same as that provided in the PSAR. The FSAR is amended near the end of waste processing operation to provide more specific information regarding deactivation. (See Integrated Safety Management Plan Table 9-5.)

[1] *Standard Format and Content for the Health and Safety Sections of License Applications for Fuel Cycle Facilities*, Regulatory Guide 3.52, Revision 2, draft, US Nuclear Regulatory Commission, Washington, DC (NRC 1995).

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
	Introduction		Executive Summary
1.0	General Information	N/A	
1.1	Facility and Process Description		Executive Summary
1.1.1	Facility Description	2.3 2.4	Facility Overview Facility Structures
1.1.2	Process Description	2.5	Process Description
1.2	Institutional Information	N/A	
1.2.1	Identity and Address	1.1	Introduction
1.2.2	Activity	N/A	
1.2.3	Site Location	1.3.1	Geography

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
1.2.4	Type, Quantity, and Form of Licensed Material	3.3.2	Hazard Identification (Vol II - V)
1.3	Site Description	1.3	Site Description
1.3.1	Geography	1.3.1	Geography
1.3.2	Demography and Land Use	1.3.2	Demography and Land Use
1.3.3	Meteorology	1.4.1	Meteorology
1.3.4	Hydrology	1.4.2	Hydrology
1.3.5	Geology and Seismicity	1.4.3	Geology
2.0	Management Organization	17	Management, Organization, and Institutional Safety Provisions
2.1	Organization and Administration	17.3	Organizational Structures, Responsibilities, and Interfaces
2.1.1	Organizational Commitments, Relationships, Responsibilities, and Authorities	17.3	Organizational Structures, Responsibilities, and Interfaces
2.1.2	Management Controls	17.4	Safety Management Policies and Programs
2.2	Safety Committees	17.4.2	Safety Review and Performance Assessments
3.0	Conduct of Operations	11	Operational Safety
3.1	Configuration Management	17.4.3	Configuration Management
3.2	Maintenance	10.5	Maintenance
3.3	Quality Assurance	14	Quality Assurance
3.3.1	Management Commitment for QA Program	14	Quality Assurance
3.3.2	Scope of QA Program	14	Quality Assurance
3.3.3	Organizational Responsibility	14	Quality Assurance
3.3.4	QA Program Description	14	Quality Assurance
3.3.5	Graded QA Approach	14	Quality Assurance
3.3.6	Application of Graded QA to SSCs and Activities	14	Quality Assurance
3.4	Training and Qualification	12	Procedures and Training
3.4.1	Organization and Management of the Training System	12.4	Training Program
3.4.2	Trainee Selection	12.4	Training Program
3.4.3	Conduct of Needs/Job Analysis and Identification of Tasks	12.4	Training Program
3.4.4	Development of Learning Objectives as the Basis for Training	12.4	Training Program

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
3.4.5	Organization of Instruction Using Lesson Plans and Other Training Guides	12.4	Training Program
3.4.6	Evaluation of Trainee Mastery of Learning Objectives	12.4	Training Program
3.4.7	Conduct of On-The-Job Training	12.4	Training Program
3.4.8	Systematic Evaluation of Training Effectiveness	12.4	Training Program
3.5	Human Factors	13	Human Factors
3.5.1	Organization and Administration	13.3	Scope of Human Factors Process
3.5.2	Human Factors and Assessment of the Correction of Deficiencies	13.4	Human Factors Program
3.6	Audits and Assessments	17.4.2	Safety Review and Performance Assessment
3.7	Incident Investigations	13.4	Human Factors Program
3.8	Records Management	17.4.4	Document Control and Records Management
3.8.1	Organization and Administration	17.4.4	Document Control and Records Management
3.8.2	Types of Records	17.4.4	Document Control and Records Management
3.8.3	Record Handling Procedures	17.4.4	Document Control and Records Management
3.8.4	Record Storage and Protection	17.4.4	Document Control and Records Management
3.9	Procedures	12.3	Procedures Program
3.10	Testing Program and Preoperational Safety Review	10.3	Commissioning
3.11	Operational Practices	11.3	Conduct of Operations
4.0	Integrated Safety Analysis	3	Hazard and Accident Analysis
4.1	Site Description	1.3	Site Description
4.2	Facility Description	2.3 2.4	Facility Overview Facility Structures
4.3	Process Description	2.5	Process Description
4.4	Process Safety Information	3.3.3.X	Hazard Evaluation
4.5	Training and Qualifications of ISA Team	3.3.1	Identification of Work
4.6	ISA Methods	3.X	Hazard and Accident Analysis
4.7	Results of the Integrated Safety Assessment	3.3.3 (Vol II - V)	Development of Control Strategies

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
4.8	Controls for Prevention and Mitigation of Accidents	3.4 (Vol II - V)	Accident Analysis Methodology
4.9	Administrative Control of the ISA		Executive Summary
5.0	Radiation Safety	7	Radiation Protection
5.1	As Low As Reasonably Achievable (ALARA) Policy	7.1	Introduction
5.2	Organizational Relationships and Personnel Qualifications	7.1	Introduction
5.3	Radiological Safety Procedures and Radiological Work Permits (RWPs)	7.1	Introduction
5.4	Training	7.1	Introduction
5.5	Ventilation systems	2.6	Confinement Systems
5.6	Air Sampling	7.1	Introduction
5.7	Contamination Control	7.1	Introduction
5.8	External Exposure	7.1	Introduction
5.9	Internal Exposure	7.1	Introduction
5.10	Summing Internal and External Exposure	7.1	Introduction
5.11	Respiratory Protection	7.1	Introduction
5.12	Instrumentation	7.1	Introduction
5.13	Integrated Safety Analysis	3.4	Accident Analysis Methodology
5.14	Radioactive Waste Management	8	Hazardous Material Protection
6.0	Nuclear Criticality Safety	6	Criticality Safety Program
6.1	NCS Technical Practices	6.3 6.4	Criticality Limits and Concerns Criticality Controls
6.1.1	Process Analysis from the Integrated Safety Analysis	6.4.6	Application of Double Contingency Principle
6.1.2	NCS Evaluations	6.4.6	Application of Double Contingency Principle
6.1.3	NCS Limits	6.4.3	Administrative Controls
6.1.4	Validation and Use of Analytical Methods	6.4.4	Methodology for Determining Criticality Limits
6.1.5	NCS Control Methods	6.4.3	Administrative Controls
6.1.6	Criticality Accident Alarm System	6.6	Criticality Instrumentation
6.2	Administrative Practices	6.5	Criticality Protection Program
6.2.1	NCS Organizational Responsibilities	6.5	Criticality Protection Program
6.2.2	Configuration Management	17.4.3.2	Configuration Management Process
6.2.3	Maintenance	6.4.3	Administrative Controls

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
6.2.4	Quality Assurance (QA)	6.4.3	Administrative Controls
6.2.5	Training	6.5.4	Criticality Safety Training and Qualifications
6.2.6	Operational Inspections, Audits, Assessments, and Investigations	6.5.5	Criticality Safety Training and Qualifications
6.2.7	Written Operating Procedures	6.5.3	Administrative Controls
6.2.8	Materials Control for NCS	N/A	
6.2.9	Emergency Preparedness	6.6	Criticality Instrumentation
7.0	Chemical Safety	8	Hazardous Material Protection
7.1	Chemical Safety Responsibility	8.3	Hazardous Material Protection and Organization
7.2	Chemical Safety Approach	8.6	Hazardous Material Exposure Control
7.3	Chemical Safety Controls	8.6	Hazardous Material Exposure Control
7.4	Hazardous Waste Management	8.6	Hazardous Material Exposure Control
8.0	Fire Safety	N/A	
8.1	Organization and Conduct of Operations	18.3	Organization and Management
8.1.1	Organization and Management	18.3	Organization and Management
8.1.2	Training and Qualifications	18.4	Training and Qualifications
8.1.3	Fire Prevention Program	18.5	Fire Prevention Program
8.2	Fire Protection Features and Systems	18.6	Fire Protection Features and Systems
8.3	Manual Fire-Fighting Capability	18.7	Manual Fire-Fighting Capability
8.4	Fire Hazard Analysis	18.8	Fire Hazard Analysis
8.5	References	N/A	
9.0	Emergency Management	15	Emergency Preparedness
9.1	Description of On-Site and Off-Site Emergency Facilities	15.4.4	Emergency Facilities and Equipment
9.2	Types of Accidents	3.3.3	Development of Control Strategies
9.3	Classification of Accidents	3.3.3	Development of Control Strategies
9.4	Detection of Accidents	15.4	Emergency Preparedness Planning
9.5	Mitigation of Consequences	15.4	Emergency Preparedness Planning
9.6	Assessment of Releases	15.4	Emergency Preparedness Planning
9.7	Responsibilities of Licensee and Other Organizational Personnel	15.4	Emergency Preparedness Planning
9.8	Notification and Coordination	15.4	Emergency Preparedness Planning
9.9	Description of the Emergency Operational Center	15.4	Emergency Preparedness Planning

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
9.10	Information to be Communicated and the Parties to be Contacted	15.4	Emergency Preparedness Planning
9.11	Public Notification	15.4	Emergency Preparedness Planning
9.12	Training	15.4	Emergency Preparedness Planning
9.13	Procedures for Safe Shutdown and Recovery	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
9.14	Drills and Exercises	15.4	Emergency Preparedness Planning
9.15	Procedures for Identifying, Locating, and Controlling Hazardous Chemicals	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
9.16	Responsibilities for Developing and Maintaining Current the Emergency Program and Its Procedures	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
10.0	Environmental Protection	9.1	Introduction
10.1	Environmental Report	N/A	
10.1.1	Description of Proposed Action	N/A	
10.1.2	Purpose of Proposed Action	N/A	
10.1.3	Description of Affected Environment	N/A	
10.1.4	Discussion of Considerations	N/A	
10.1.5	Analysis of Environmental Effects of Proposed Action and Alternatives	N/A	
10.1.6	Federal and State Environmental Requirements	9.1.1 9.4	Permit Overview Radioactive and Hazardous Waste Processes
10.2	Environmental Safety Program	9.3	Radioactive and Hazardous Waste Management Program and Organization
10.2.1	Features for Contamination Control	2.3	Facility Overview
10.2.2	Environmental Monitoring Program	9.1 9.4	Introduction Radioactive and Hazardous Waste Processes
10.2.3	Emergency Plan	15.X	
10.2.4	Maintenance and Surveillance	9.3	Radioactive and Hazardous Waste Management Program and Organization
10.2.5	Configuration Management	17.4.3.2	Configuration Management Process
10.2.6	Organization and Management	9.3.1 17	Program Summary Management, Organization, and Institutional Safety Provisions
10.2.7	Quality Assurance	14.1	Introduction

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
10.2.8	Training	9.3 9.7 (ERPP)	Radioactive and Hazardous Waste Management Program and Organization Environmental Radiological Protection Plan (ERPP)
10.2.9	Event Notification and Reporting	9.1.1	Permit Overview
10.2.10	Bibliography	9.8	References
11.0	Decommissioining	16	Deactivation and Decommissioning
11.1	Conceptual Decommissioning Plan	16.1	Introduction
11.1.1	Information for Conceptual Decommissioning Plan	16.4	Deactivation Requirements
11.1.2	Information for Total or Partial Cessation of Operations	16.5	Transition Readiness
11.1.3	Bibliography	16.7	References
11.1.4	Appendix A: Cost Estimating Tables	N/A	
11.2	Decommissioning Funding Plan and Financial Assurance Mechanisms	N/A	
11.2.1	Decommissioning Cost Estimate	N/A	
11.2.2	Financial Assurance Mechanism(s)	N/A	
11.2.3	Updating the Cost Estimate and Funding Level	N/A	
11.2.4	Bibliography	N/A	
11.2.5	Appendix A: Sample Sight Draft	N/A	
Appendix A	Radiation Protection Program Outline	7 RPP	Radiation Protection
Appendix B	Environmental Radiation Protection Program Outline	9.5 ERPP	Environmental Radiation Protection Plan (ERPP)

The SARs should include multiple volumes. Volume I should provide information that is applicable to more than one of the facilities (e.g., Pretreatment, Low-Activity Waste Vitrification, High-Level Waste Vitrification, and Balance of Facilities). Other volumes should be facility specific and contain, at a minimum, chapters 2, 3, 4, and 5.

Executive Summary

- **E.1 Facility Background and Mission**
- **E.2 Facility Overview**
- **E.3 Facility Hazard Classification**
- **E.4 Safety Analysis Overview**
- **E.5 Organization**
- **E.6 Safety Analysis Conclusions**
- **E.7 SAR Organization**
- **E.8 Summary of Significant Changes from the Preliminary Safety Analysis Report (FSAR stage)**

1 Site Characteristics

- **1.1 Introduction**
- **1.2 Requirements**
- **1.3 Site Description**
- **1.4 Environmental Description**
- **1.5 Natural Phenomena Hazards**
- **1.6 External Man-Made Threats**
- **1.7 Nearby Facilities**
- **1.8 References**

2 Facility Description

- **2.1 Introduction**
- **2.2 Requirements**
- **2.3 Facility Overview**
- **2.4 Facility Structures**
- **2.5 Process Description**
- **2.6 Confinement Systems**
- **2.7 Safety Support Systems**
- **2.8 Utility Distribution Systems**
- **2.9 Auxilliary Systems and Support Facilities**
- **2.10 References**

3 Hazard and Accident Analyses
- **3.1 Introduction**
- **3.2 Requirements**
- **3.3 Hazard Analysis Methodology**
- **3.4 Accident Analysis Methodology**
- **3.5 Hazard Classification**
- **3.6 Common Cause and Common Mode Design Basis Events**
- **3.7 Seismic Probabilistic Risk Assessment**
- **3.8 Adherence to Risk Goals and Results**
- **3.9 References**

4 Important to Safety Structures, Systems, and Components
- **4.1 Introduction**
- **4.2 Requirements**
- **4.3 Safety Design Class Systems, Structures, and Components**
- **4.4 Safety Design Significant Systems, Structures, and Components**
- **4.5 References**

5 Derivation of Technical Safety Requirements
- **5.1 Introduction**
- **5.2 Requirements**
- **5.3 Technical Safety Requirement Coverage**
- **5.4 Derivation of Facility Modes**
- **5.5 Technical Safety Requirement Derivation**
- **5.6 Design Features**
- **5.7 Interface with TSRs from Other Facilities**
- **5.8 References**

6 Criticality Safety Program
- **6.1 Introduction**
- **6.2 Requirements**
- **6.3 Criticality Limits and Concerns**
- **6.4 Criticality Controls**
- **6.5 Criticality Protection Program**
- **6.6 Criticality Instrumentation**
- **6.7 References**

7 Radiation Protection
- **7.1 Introduction**
- **7.2 Requirements**
- **7.3 References**

8 Hazardous Material Protection
- **8.1 Introduction**
- **8.2 Requirements**
- **8.3 Hazardous Material Protection and Organization**
- **8.4 ALARA Policy and Program**
- **8.5 Hazardous Material Training**
- **8.6 Hazardous Material Exposure Control**
- **8.7 Hazardous Material Monitoring**
- **8.8 Hazardous Material Protection Instrumentation**
- **8.9 Hazardous Material Protection Record Keeping**
- **8.10 Hazard Communication Program**
- **8.11 Occupation Chemical Exposures**
- **8.12 References**

9 Waste Management
- **9.1 Introduction**
- **9.2 Requirements**
- **9.3 Radioactive and Hazardous Waste Management Program and Organization**
- **9.4 Radioactive and Hazardous Waste Processes**
- **9.5 Waste Sources and Characteristics**
- **9.6 Waste Handling or Treatment Systems**
- **9.7 Environmental Radiological Protection Plan**
- **9.8 References**

10 Initial Testing, In-Service Surveillance, and Maintenance
- **10.1 Introduction**
- **10.2 Requirements**
- **10.3 Commissioning**
- **10.4 Surveillance Program**
- **10.5 Maintenance**
- **10.6 References**

11 Operational Safety
- **11.1 Introduction**
- **11.2 Requirements**
- **11.3 Conduct of Operations**

12 Procedures and Training
- **12.1 Introduction**
- **12.2 Requirements**
- **12.3 Procedures Program**
- **12.4 Training Program**
- **12.5 References**

13 Human Factors
- **13.1 Introduction**
- **13.2 Requirements**
- **13.3 Scope of Human Factors Process**
- **13.4 Human Factors Programmatic Interactions**
- **13.5 Optimization of Human Factors Elements**
- **13.6 References**

14 Quality Assurance
- **14.1 Introduction**
- **14.2 Requirements**
- **14.3 References**

15 Emergency Preparedness
- **15.1 Introduction**
- **15.2 Requirements**
- **15.3 Scope of Emergency Preparedness Program**
- **15.4 Emergency Preparedness Planning**
- **15.5 References**

16 Deactivation and Decommissioning
- **16.1 Introduction**
- **16.2 Requirements**
- **16.3 Design and Operational Features**
- **16.4 Deactivation Requirements**
- **16.5 Transition Readiness**
- **16.6 Turning Over WTP Facilities to DOE**
- **16.7 References**

17 Management, Organization, and Institutional Safety Provisions
- **17.1 Introduction**
- **17.2 Requirements**
- **17.3 Organizational Structures, Responsibilities, and Interfaces**
- **17.4 Safety Management Policies and Programs**
- **17.5 References**

18 Fire Protection
- **18.1 Introduction**
- **18.2 Requirements**
- **18.3 Organization and Management**
- **18.4 Training and Qualification**
- **18.5 Fire Prevention Program**
- **18.6 Fire Protection Features and Systems**
- **18.7 Manual Fire-Fighting Capability**
- **18.8 Fire Hazard Analysis**
- **18.9 Fire Protection for Filter Plenums**

4.0 References

BNI, 2001. *Safety Requirements Document Volume II*, 24590-WTP-SRD-ESH-01-001-02. Bechtel National, Inc., Richland, Washington.

DOE-ORP, 2000. Contract No. DE-AC27-01RV14136, December 2000. US Department of Energy, Office of River Protection, Richland, Washington.

DOE-RL, 1998a. *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0003, Revision 1. US Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL, 1998b. *Top-Level Radiological, Nucelar, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 1. US Department of Energy, Richland Operations Office, Richland, Washington.

NRC, 1994. *Integrated Safety Analysis Guidance Document*, draft NUREG-1513, distributed 8 August 1994, US Nuclear Regulatory Commission, Washington, DC.

NRC, 1995. Regulatory Guide 3.52, *Standard Format and Content for the Heatlh and Safety Sections of License Applications for Fuel Cycle Facilities*, draft Revision 2, US Nuclear Regulatory Commission, Washington, DC.

Document title:	**Integrated Safety Management Plan**
Contract number:	DE-AC27-01RV14136
Department:	Environmental, Safety, and Health
Document number:	24590-WTP-ISMP-ESH-01-001, Rev 0e
Date of issue:	19 February 2002
Issue status:	Approved

History Sheet

Rev	Date	Reason for revision	Revised by
0	29 Aug 2001	Supersedes BNFL-5193-ISP-01 Revision 7. Incorporates 24590-WTP-ABCN-ESH-01-017 changes, a WTP contractor-approved change notice.	R Dickey
0a	24 Sep 2001	Incorporated 24590-WTP-ABCN-ESH-01-011 Rev 0 changes (contractor-approved ABCN), and added two acronyms and one reference that were defined in text added by the referenced ABCN.	R Dickey
0b	4 Oct 2001	Incorporates ABCN-24590-01-00006 Rev 0 changes as partially approved by DOE Letter 01-OSR-0311 (CCN 023253) and contractor approved as revised ABCN-24590-01-00006, Rev 1.	R Dickey
0c	27 Dec 2001	Incorporates 24590-WTP-ABCN-ESH-01-023 Rev 0 changes (contractor-approved ABCN).	R Dickey
0d	28 Dec 2001	Incorporates 24590-WTP-ABCN-ESH-01-011 Rev 1 changes (contractor-approved ABCN).	R Dickey
0e	19 Feb 2002	Incorporates ABCN-24590-01-00004 Rev 2 changes as approved by DOE Letter 02-OSR-0034 (CCN 028170).	R Dickey

Revision Status

Page No.	Rev	Page No.	Rev	Page No.	Rev	Page No.	Rev
i	0e	1-21	0d	3-22	0b	4-15	0e
ii	0e	1-22	0a	3-23	0	4-16	0e
iii	0e	1-23A	0d	3-24	0	4-17	0e
iv	0e	1-23B	0a	3-25	0	4-18	0e
v	0	1-23C	0b	3-26	0	4-19	0e
vi	0	1-24	0	3-27	0	4-20	0e
vii	0	2-1	0	3-28	0	4-21	0e
viii	0	2-2	0	3-29	0	4-22	0e
ix	0e	2-3	0	3-30	0	4-23	0
x	0a	2-4	0	3-31	0	4-24	0
xi	0	2-5	0	3-32	0	5-1	0b
xii	0	3-1	0	3-33	0	5-2	0
1-1	0	3-2	0	3-34	0	5-3	0
1-2	0	3-3	0	3-35	0	5-4	0
1-3	0	3-4	0	3-36	0	5-5	0
1-4	0	3-5	0	3-37	0b	5-6	0
1-5	0	3-6	0e	3-38	0	5-7	0
1-6	0	3-7	0	3-39	0	5-8	0b
1-7	0	3-8	0	4-1	0	5-9	0
1-8	0	3-9	0	4-2	0	5-10	0
1-9	0b	3-10	0	4-3	0	5-11	0
1-10	0	3-11	0	4-4	0	5-12	0b
1-11	0	3-12	0	4-5	0	6-1	0
1-12	0	3-13	0	4-6	0	6-2	0
1-13	0	3-14	0	4-7	0	6-3	0
1-14	0b	3-15	0	4-8	0	7-1	0
1-15	0	3-16	0	4-9	0e	7-2	0
1-16	0	3-17	0	4-10	0e	7-3	0
1-17	0b	3-18	0	4-11	0e	8-1	0
1-18	0	3-19	0	4-12	0e	8-2	0
1-19	0	3-20	0	4-13	0e	8-3	0
1-20	0	3-21	0a	4-14	0e	9-1	0

Page No.	Rev	Page No.	Rev	Page No.	Rev	Page No.	Rev
9-2	0	10-1	0	11-7	0	12-4	0
9-3	0	10-2	0	11-8A	0c	12-5	0
9-4	0	10-3	0	11-8B	0c	12-6	0
9-5	0	10-4	0	11-9	0	12-7	0b
9-6	0	11-1	0	11-10	0	12-8	0
9-7	0	11-2	0c	11-11	0c	13-1	0
9-8	0	11-3	0c	11-12	0	13-2A	0a
9-9	0	11-4	0	12-1	0	13-2B	0e
9-10	0	11-5	0	12-2	0	13-3	0
9-11	0b	11-6	0	12-3	0		

Approved by: _____ _____ Date: _____
(Print name) (Sign)

CONTENTS

Acronyms vii
1.0 Project Safety Approach 1-1
1.1 Introduction 1-1
1.2 Summary 1-3
1.3 Description of the Integrated Safety Management Plan 1-6
1.3.1 Project Initiation 1-6
1.3.2 Laws/Regulations/Top-Level Safety Requirements/Best Industry Practices 1-7
1.3.3 Safety Requirements 1-7
1.3.4 Process Hazards Analysis 1-8
1.3.5 Facility Design/Development Activities and Safety Features Identification 1-9
1.3.6 Accident Analysis 1-9
1.3.7 Acceptable Level of Public Safety 1-10
1.3.8 Acceptable Level of Worker Safety 1-13
1.3.9 Quality Assurance Program 1-15
1.3.10 Classification of Structures, Systems, and Components 1-16
1.3.11 Quality Levels 1-19
1.3.12 Training 1-19
1.3.13 Procedures 1-20
1.3.14 Commissioning 1-21
1.3.15 Operations 1-21
1.3.16 Configuration Management 1-22
1.3.17 Incident Investigations 1-24
1.3.18 Emergency Planning 1-25
1.3.19 Deactivation 1-25
2.0 Compliance with Laws and Regulations 2-1
2.1 Statutory Compliance 2-1
2.2 Compliance with 10 CFR 830.120, “Quality Assurance Requirements” 2-2
2.3 Compliance with 10 CFR 835, “Occupational Radiation Protection” 2-3
2.3.1 Implementation of 10 CFR 835 2-3
2.3.2 Potential Exemption Request (this section has been deleted) 2-4
2.3.3 Radiation Protection Program 2-4
2.4 Environmental Radiation Protection Program 2-5
2.5 Compliance with 10 CFR 820, ‘Procedural Rules for DOE Nuclear Facilities’ 2-6
3.0 Conformance to Top-Level Safety Standards and Principles 3-1
3.1 Defense-In-Depth 3-1
3.1.1 Approach to Defense-in-Depth 3-1
3.2 Safety Responsibilities 3-4
3.3 Authorization Basis 3-5
3.3.1 Content of the Authorization Basis 3-5
3.3.2 Control of the Authorization Basis 3-9

3.3.3 Changes to the Authorization Basis 3-9
3.4 Safety/Quality Culture 3-14
3.5 Quality Assurance Program (QAP) 3-15
3.6 Facility Design for Postulated Events 3-16
3.6.1 Normal Operations 3-16
3.6.2 Anticipated Operational Occurrences 3-17
3.6.3 Accidents 3-17
3.7 Proven Engineering Practices 3-18
3.7.1 Passive Features 3-19
3.7.2 Active Features 3-19
3.8 Criticality Safety 3-20
3.9 Radiation Protection Practices 3-21
3.9.1 Radiation Protection Design 3-21
3.9.2 ALARA Design 3-22
3.10 Emergency Preparedness 3-23
3.11 Safety Systems Design 3-24
3.12 Human Factors 3-27
3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI) 3-29
3.14 Commissioning and Operation 3-31
3.15 Training and Qualification 3-32
3.16 Internal Safety Oversight 3-34
3.16.1 Safety Committees 3-35
3.16.2 Safety Improvement Program 3-37
3.16.3 Incident Investigations 3-38
3.16.4 Unreviewed Safety Questions 3-38
3.16.5 Performance Monitoring 3-39
3.16.6 Performance Indicators 3-40
3.16.7 Lessons Learned 3-40
3.16.8 Feedback and Trending 3-40
4.0 Standards-Based Management 4-1
4.1 Safety Management Processes 4-1
4.1.1 Development of Safety Management Processes 4-1
4.1.2 Identification of Safety Management Program Drivers 4-3
4.1.3 Development of Safety Management Programs 4-4
4.1.4 Compliance to and Maintenance of Safety Management Programs 4-5
4.2 Tailoring Safety Management Processes 4-8
4.2.1 Engineered Features 4-9
4.2.2 Training and Procedures 4-9
4.2.3 Tailoring of Safety-Related Documentation 4-9
5.0 Process Safety Management 5-1
5.1 Process Safety Information 5-1

5.2 Control of Subcontractors 5-3
5.3 Configuration Management 5-5
5.4 Compliance Audits 5-6
5.5 Process Hazards Analysis 5-6
5.6 Conformance to Other Top-Level Safety Standards and Principles 5-7
5.6.1 Procedure Development 5-8
5.6.2 Updating of the Hazard Analysis Report 5-8
5.6.3 Development of the Operator Training Program 5-9
5.6.4 Commissioning Review 5-9
5.6.5 Mechanical Integrity 5-10
5.6.6 Hot Work Operations 5-11
5.6.7 Investigations of Incidents 5-11
5.6.8 Emergency Action Plan 5-13
6.0 Integrated Safety Management 6-1
6.1 Integration Into Work Planning and Performance 6-1
6.1.1 Line Management Responsibility for ES&H 6-2
6.1.2 Lines of Authority and Responsibility 6-2
6.1.3 Personnel Qualification and Resources 6-2
6.1.4 Hazard Assessments, Controls, and Operating Conditions 6-3
7.0 Regulatory Interfaces 7-1
7.1 Environmental Protection Interface 7-1
7.2 Occupational Health and Safety Interface 7-2
7.3 Safeguards and Security Interface 7-2
7.4 Resolution of Conflicting Requirements and Standards 7-3
8.0 Document Control and Maintenance 8-1
9.0 Scheduling of Safety-Related Activities 9-1
9.1 Scheduling Safety-Related Activities 9-1
9.2 Scheduling of Events for Regulatory Submittals 9-1
9.3 Flow of Safety-Related Work and Deliverables 9-11
10.0 Assessments 10-1
10.1 Management Assessments 10-2
10.2 Independent Assessments 10-2
10.3 Corrective Action Implementation and Tracking 10-3
10.4 Support of DOE Inspection and Corrective Action/Enforcement Action Programs 10-3
10.4.1 DOE Inspection Program 10-3
10.4.2 DOE Corrective Action/Enforcement Action Program 10-4
11.0 Organization Roles, Responsibilities, and Authorities 11-1
11.1 Interim Design Project 11-1
11.2 Operations Phase 11-8

12.0 Definitions 12-1
13.0 References 13-1

FIGURES

1-1 Project Safety Approach 1-5
1-2 Location of Public Receptor 1-12
1-3 Location of Facility and Collocated Workers 1-14
4-1 Safety Management Processes 4-2
4-2 SRD Link to Design 4-6
4-3 SRD Change Process 4-7
9-1 Sequence of Safety Related Activities 9-2
11-1 Management Structure and Organization for the BNI Design, Construction, and Commissioning Contract 11-3

TABLES

1-1 BNFL Team Experience Related to the TWRS-P Project (this table has been deleted) 1-2
1-2 Radiological Exposure Standards Above Normal Background 1-10
1-3 Responsibilities for Changes to the RPP-WTP. 1-24
3-1 Outline And Content of Emergency Response Plan 3-25
4-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 (this table has been deleted) 4-10
4-2 Planned Differences Between PSAR and FSAR Content (this table has been deleted) 4-14
8-1 Safety Management Records 8-1
9-1 Key Safety-Related Activities – Design Phase 9-5
9-2 Key Safety-Related Activities – Fabrication and Construction Phase. 9-7
9-3 Key Safety-Related Activities – Commissioning Phase. 9-8
9-4 Key Safety-Related Activities – Operations Phase. 9-9
9-5 Key Safety-Related Activities – Deactivation Phase 9-10

Acronyms

AB	Authorization Basis
AIChE	American Institute of Chemical Engineers
AIHA	American Industrial Hygiene Association
ALARA	As Low As Reasonably Achievable
BNI	Bechtel National, Inc.
CAMS	Corrective Action Management System
CAR	Construction Authorization Request
CFR	Code of Federal Regulations
Ci	Curie
CM	Configuration management
CM Plan	RPP-WTP Configuration Management Plan
DAR	Deactivation Authorization Request
DBE	Design Basis Earthquake OR Design Basis Event
DC&C	Design, Construction, and Commissioning
DCD	Design Criteria Database
DOE	U.S. Department of Energy
DOELAP	DOE Laboratory Accreditation Program
DOE-RL	U.S. Department of Energy Richland Operations Office
DOH	Washington State Department of Health
DWPF	Defense Waste Processing Facility
EAL	Emergency Action Level
Ecology	Washington State Department of Ecology
ECP	Employee Concerns Program
EDSP	Engineering Design Safety Principle
EIS	Environmental Impact Statement
EMP	Emergency Management Program
EMS	Emergency Management System
EP	Emergency Plan
EPA	U.S. Environmental Protection Agency
EPIP	Emergency Plan Implementing Procedure
ER	Environmental Report
ERPG	Emergency Response Planning Guide
ERPP	Environmental Radiation Protection Program
ES&H	Environment, Safety, and Health
FHA	Fire Hazard Analysis
FR	Federal Register
FSAR	Final Safety Analysis Report
HAL	Highly Active Liquids
HAR	Hazard Analysis Report
HAZOP	Hazard and Operability (analysis)
HEPA	High-Efficiency Particulate Air (filter)
HLW	High-Level Waste
HRC	Hazards Research Corporation
Hwy	Highway
ICBO	International Conference of Building Officials
IPT	Integrated Product/Process Team

IRT	Independent Review Team
ISA	Integrated Safety Analysis
ISAR	Initial Safety Analysis Report
ISMP	Integrated Safety Management Plan
ISO	International Organization of Standards
ITS	Important to Safety
LAW	Low-Activity Waste
LWA	Limited Work Authorizations
MSDS	Material Safety Data Sheets
NAICS	North American Industry Classification System
NCRP	National Council on Radiation Protection and Measurements
NPH	Natural Phenomenon Hazard
NRC	U.S. Nuclear Regulatory Commission
NVLAP	National Voluntary Laboratory Accreditation Program
OAR	Operating Authorization Request
OPM	Operational Preventive Measures
OSHA	Occupational Safety and Health Administration
PFD	Process Flow Diagram
PHA	Process Hazards Analysis
PHMC	Project Hanford Management Contractor
PSAR	Preliminary Safety Analysis Report
PSC	Project Safety Committee
PSM	Process Safety Management
QA	Quality Assurance
QAM	Quality Assurance Manual
QAP	Quality Assurance Program
QAPIP	Quality Assurance Program and Implementation Plan
QARD	Quality Assurance Requirements and Description
QL	Quality Level
RAMI	Reliability, Availability, Maintainability, and Inspectability
RCRA	*Resource Conservation and Recovery Act of 1976*
rem	Roentgen-Equivalent Man
RG	Regulatory Guide
RL	Department of Energy Richland Operations Office
RMP	Risk Management Plan
RPP	Radiation Protection Program
RPP-WTP	River Protection Project – Waste Treatment Plant
SAR	Safety Analysis Report
SDC	Safety Design Class
SDS	Safety Design Significant
SER	Safety Evaluation Report
SIXEP	Site Ion Exchange Effluent Plant
SNM	Special Nuclear Material
SPD	System Performance Demonstrations
SRD	Safety Requirements Document
SSC	Structures, Systems, and Components
STD	Standard (also Std)

TSR	Technical Safety Requirement
TEDE	Total Effective Dose Equivalent
TWRS	Tank Waste Remediation System
TWRS-P	Tank Waste Remediation System-Privatization
UBC	Uniform Building Code
USC	United States Code
USQ	Unreviewed Safety Question
VPP	Voluntary Protection Program
VSL	Vitreous State Laboratory
WAC	*Washington Administrative Code*
WISHA	Washington Industrial Safety and Health Administration

1.0 Project Safety Approach

The RPP-WTP Contractor's safety approach is implemented with the recognition that the defined work for processing and immobilizing Hanford tank waste involves inherent radiological and chemical hazards from which hazardous situations may arise. The RPP-WTP Contractor is committed to integrating the development of safety criteria and design requirements, the hazard analysis and accident analysis process, and the facility design to minimize the risk associated with these hazards and hazardous situations. The RPP-WTP Contractor accepts responsibility for the safety of the RPP-WTP and for adequate protection of the health and safety of the public, worker safety, environmental protection, and compliance with applicable laws and regulations.

This chapter of the Integrated Safety Management Plan (ISMP) provides an overview of the RPP-WTP design, construction, and commissioning (DC&C) Contractor (i.e., Bechtel National, Inc. [BNI]) safety approach developed for the River Protection Project – Waste Treatment Plant (RPP-WTP). The elements of this approach, through their evolutionary implementation in Part A of the project, form the bases for this ISMP. The ISMP is followed and will be further developed during Part B of the Project for detailed design, construction, operation, and deactivation of the facility.

The Project safety approach is summarized in Section 1.1, "Introduction". The components of the safety approach are described in greater detail in Section 1.2, "Summary". The elements of the safety approach are described in Section 1.3, "Description of the Integrated Safety Management Plan".

1.1 Introduction

The safety management practices outlined in the ISMP have been developed specifically for the Project. The development of these management practices was based on the experience of the Project team at other nuclear facilities in the areas of design, construction, and operation. These practices ensure implementation of the corporate policy that no activities are more important than the health and safety of its workers, contractors, the public, or protection of the environment.

The ISMP documents the process by which laws, regulations, and standards applicable to the nuclear, radiological, and process safety aspects of the Project are incorporated into programs for facility design, construction, operation, and deactivation to ensure adequate safety of workers and the public and protection of the environment. A further role of the ISMP is to demonstrate how practices are in line with the RPP-WTP Contractor policies to ensure that the safety culture achieved at other nuclear chemical facilities can be successfully sustained through the different phases of the RPP-WTP. At this stage in the project, the ISMP is biased towards the design and construction phase, during which most of the processes described are developed. However, the principles of the ISMP for later stages of the facility life through operation and deactivation and how the design and construction phase will be integrated into these later stages is discussed. The ISMP also describes how the safety management practices will be followed and further developed during Part B of the Project.

Table 1-1 BNFL Team Experience Related to the TWRS-P Project (this table has been deleted)

To accomplish its roles, the ISMP describes the following:

1) The facility defined work to process and immobilize Hanford Tank waste in a safe manner (ISMP Section 1.3.1, "Project Initiation")
2) The selection of a safe and proven technology (ISMP Section 3.7, "Proven Engineering Practices")
3) The development and use of the SRD (ISMP Section 1.3.3, "Safety Requirements Document")
    a) To establish the Safety Criteria by which the process hazard analysis (PHA) and accident analysis identify features required for worker and public safety
    b) To identify the design requirements that, when implemented, ensure that prevention and mitigation controls will perform their specified safety functions
4) The use of PHA to identify the full range of potential radiological and chemical hazards and hazardous situations (ISMP Section 1.3.4, "Process Hazards Analysis")
5) The accident analyses performed to identify engineered and administrative controls required for worker and public safety (ISMP Section 1.3.6, "Accident Analysis")
6) The iteration of the PHA, accident analyses, and design to ensure an adequate level of safety for the workers and the public (ISMP Sections 1.3.7, "Acceptable Level of Public Safety" and 1.3.8, "Acceptable Level of Worker Safety")
7) The development of the technical safety requirements, if required, that are based on:
    a) A process variable, design feature, or operating restriction that is an initial condition (i.e., the assumed facility state) for an accident analysis
    b) Structures, systems, and components that must function to maintain compliance with public and worker radiological and chemical exposure standards
8) The development of procedures and training to achieve and maintain the required administrative controls (ISMP Sections 1.3.12, "Training" and 1.3.13, "Procedures")
9) The development of an emergency preparedness program and implementing procedures (ISMP, Section 1.3.18, "Emergency Planning")
10) The assignment of design, construction, and operational roles and responsibilities and the use of assessments to ensure the necessary attributes of the ISMP are effectively accomplished (ISMP, Chapters 10.0, "Assessments", and 11.0, "Organizational Roles, Responsibilities, and Authorities")

Chapter 1.0 of the ISMP presents the BNI safety approach. Chapters 2.0 through 11.0 are formatted to correspond to the attributes included in RL/REG-97-07, *Guidance for the Review of TWRS Privatization Contractor Integrated Safety Management Plan Submittal Package* (DOE-RL 1997).

Throughout the ISMP, lists of items are numbered for the convenience of the reviewers in referring to individual items. The numbering is not an indication of the importance or sequence of the items.

Chapter 12.0, "Definitions", contains the definitions of some of the terms, phrases, or documents that are found throughout the ISMP. When used unmodified in the ISMP, "worker" refers to the facility and collocated worker, both individually and collectively.

Within this document, the *Safety Requirements Document* (SRD) (BNI 2001b and BNI 2001c), *Hazard Analysis Report* (HAR) (BNFL 1997b), *Quality Assurance Program* (QAP) (BNFL 1997a, BNFL 1998c), *Quality Assurance Manual* (QAM) (BNI 2001), and *Initial Safety Analysis Report* (ISAR) (BNI 2001d and 2001e), are cited using acronyms. Full reference information for these documents appears in Chapter 13.0, "References".

1.2 Summary

The Project safety approach is implemented with the recognition that the defined work of processing and immobilizing Hanford tank waste involves inherent radiological and chemical hazards from which hazardous situations may arise. The Project is integrating the development of Safety Criteria, design requirements, the hazard analysis and accident analysis processes, and the facility design to minimize the risk associated with these hazards and hazardous situations. The elements of this approach, through their evolutionary implementation in Part A of the Project, form the bases for this ISMP.

The safety approach for the Project is based on applying best industry practices and cost-effective processes that come from successful and safe operation in the commercial nuclear environment and the chemical process industry. The purpose of the safety approach is to achieve the following objectives.

1) Ensure an adequate level of safety at the facility for the workers and the public.
2) Comply with applicable laws and regulations.
3) Conform to top-level safety standards and principles stipulated by the U.S. Department of Energy (DOE-RL 1996b).

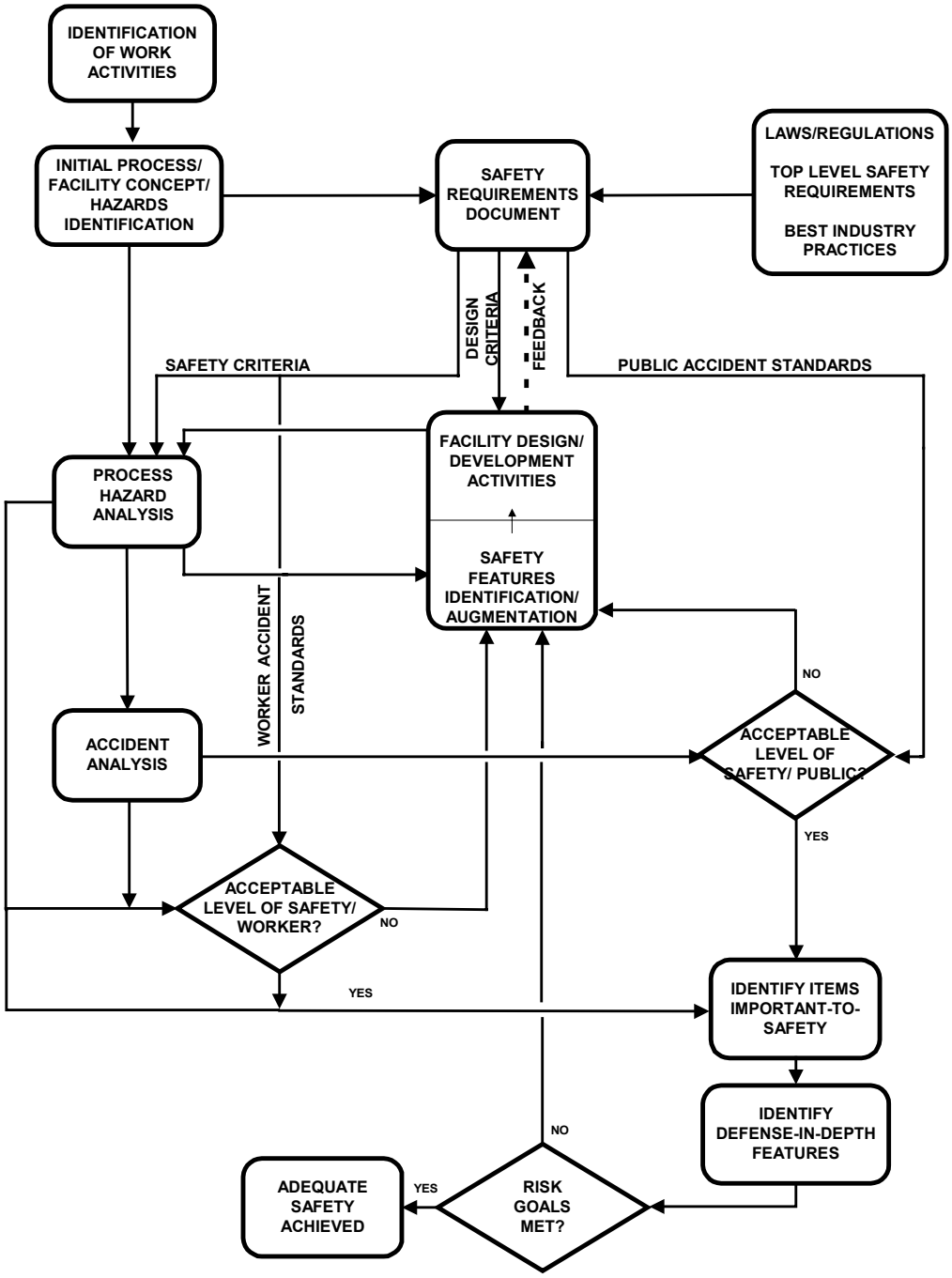
A diagram of the Project safety approach is presented in Figure 1-1. The safety approach begins with the definition of the work to be performed and continues with the development of the conceptual process flow diagrams (PFD) and other facility design information required to accomplish the defined work. The PFDs and design development give consideration to the types of work to be accomplished, the hazards identified for similar facilities, and the methods by which these hazards were previously eliminated or controlled for similar facilities. This conceptual information is used to identify appropriate hazards-based standards and initiate the development of the SRD.

The identification of hazards and hazardous situations helps to characterize the hazardous situations as those that may require prevention or mitigation. The identification and characterization of the hazards and hazardous situations establish a basis for describing approaches and measures to control the hazards. Safety Criteria are then developed that document the set of standards and requirements necessary to ensure implementation of the necessary hazard control strategies. These Safety Criteria are documented in the SRD and are based on applicable laws and regulations, the U.S. Department of Energy's (DOE) top-level safety requirements, and best industry practices. The SRD provides Safety Criteria to the PHA by which an initial assessment of the adequacy of the design is made.

As accident prevention and mitigation safety features are identified in the PHA, the resulting facility design impacts are fed back to the SRD process, as required, for further development of more detailed Safety Criteria and design requirements to ensure all safety features provide their specified safety functions.

As the PHA, PFDs, and facility design mature, accident analyses are performed to confirm judgements made during the PHA and to further characterize the accident scenarios to demonstrate compliance with radiological and chemical exposure standards for accidents. Additional protection for workers is identified by the PHA, the accident analyses, and the application, as appropriate, of Process Safety Management (PSM) required by 29 CFR 1910.110.

Figure 1-1 Project Safety Approach



Significant features of the Project safety approach are described as follows.

1) The approach continually integrates hazard identification, SRD development, design development, and accident analysis throughout the facility design, construction, operation, and deactivation phases.
2) The approach uses the best industry practices that include PHA, a rigorous design process based on a set of credible accidents and a defense-in-depth philosophy, and verification of the level of facility safety through accident analysis and validation of requirements implementation.
3) The PHA identifies and evaluates the significance of potentially hazardous situations. For each identified event, a defense-in-depth approach applies a level of protection in terms of engineered features and administrative controls that is commensurate with the severity of the unmitigated event. The hazards evaluation techniques satisfy the requirements of a hazards analysis process established by the American Institute of Chemical Engineers (AIChE 1992).
4) A conservative approach to accident consequence analysis is used in terms of input assumptions, boundary conditions, and modeling techniques. As the process and facility design mature, the modeling is refined to eliminate unnecessary conservatism. This strategy is consistent with risk-based approaches that allow the use of uncertainty analysis to better identify the impact of assumptions and state of knowledge on results from the safety analyses.
5) The safety approach documents how the identification of the engineered and administrative controls credited for public and worker safety and facility Safety Criteria is accomplished.

This approach to safety analysis is similar to that described in draft NUREG 1513, *Integrated Safety Analysis Guidance Document,* (NRC 1994) published by the U.S. Nuclear Regulatory Commission (NRC).

1.3 Description of the Integrated Safety Management Plan

Each of the elements of the safety approach are described in detail in the following sections.

1.3.1 Project Initiation

The Project safety approach began with a discussion to aid in understanding of the work to be accomplished and the development of the conceptual design of the processes and facility to accomplish this work. The development of the conceptual design considered the work to be performed, hazards and hazardous situations identified for similar facilities, and the methods to eliminate or control these hazards and hazardous situations. Early in the development of the conceptual design, hazards identification and evaluation techniques appropriate for the preliminary nature of the process and facility design were selected and applied.

1.3.2 Laws/Regulations/Top-Level Safety Requirements/Best Industry Practices

Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors, DOE/RL-96-0006 (DOE-RL 1996b) provides a set of top-level radiological, nuclear, and process safety standards and principles prescribed by DOE for accomplishing the required level of safety for the RPP-WTP. This document is used as one resource for the development of the SRD. Included in DOE/RL-96-0006 are radiological exposure and risk standards for evaluation of normal and offnormal events. Additional resources for the identification of standards were derived from the U.S. and United Kingdom (UK) commercial nuclear and chemical industries. The identification of the remaining requirements is described in the following section.

1.3.3 Safety Requirements

The SRD defines the Safety Criteria and the design requirements (implementing codes and standards) necessary to protect the public and workers from radiological, nuclear, and process hazards and hazardous situations. The Safety Criteria and codes and standards of the SRD are applied to the RPP-WTP. The SRD, as well as the ISMP, applies to Project contractors. By application of the SRD and ISMP to all Project activities, a consistent project-wide approach is applied to Environmental, Safety, and Health (ES&H) matters. The hazards and hazardous situations at the facility will change significantly throughout the construction, operation, and deactivation phases of the Project. The SRD was developed by an iterative process that will continue as the design matures through the construction, commissioning, operation, and deactivation of the facility. The development involved identifying the work to be performed, identifying hazards and hazardous situations of the facility operation by the PHA and accident analyses, reviewing of pertinent regulations and industry practices, and identifying engineered and administrative controls.

Once the work activity was identified for the Project and the hazards associated with this work determined, the Safety Criteria were defined by the requirements necessary to ensure protection of the public and workers from radiological, nuclear, and process hazards. The Safety Criteria are based on the following:

1) Mandated regulatory requirements (statutory and contractual; including those identified as top-level safety requirements [standards and principles]) and equivalent requirements
2) Requirements and guidance documents deemed relevant to waste management facilities such as this Project
3) Best industry practices from the government, commercial nuclear, and chemical industries

The engineered and administrative controls necessary to eliminate and control hazards and hazardous situations are established via the PHA, the accident analysis, and the necessary level of protection required to satisfy the SRD Safety Criteria. Once the controls are selected, the SRD identifies the implementing codes and standards necessary to ensure that engineered and administrative controls are properly designed, implemented, and maintained. The requirements, guidance documents, and practices are incorporated into the SRD, tailored toward applicability to RPP-WTP operations, the control of hazards, and the adequacy to protect public and worker health and safety. These codes and standards are used by the appropriate organizations to ensure that the design, construction, testing, and maintenance of Important-to-Safety SSCs are such that they can perform their specified public and worker safety functions when required. Additional detail on the SRD and definition of Important-to-Safety is provided in ISMP Section 4.1, "Safety Management Processes" and Section 1.3.10, "Classification of Structures, Systems, and Components".

1.3.4 Process Hazards Analysis

The PHA process is a systematic team-based approach used to identify and analyze the significance of potentially hazardous situations associated with the operation and maintenance of the RPP-WTP. Other hazardous situations unique to the deactivation phase will be identified near the end of waste processing operations. The PHA process includes preliminary hazard analysis and Hazard and Operability (HAZOP) Analysis. The process is enhanced by the experience gained by the Project team from similar analyses performed at similar facilities. The PHA is performed to ensure the facility is designed to provide accident prevention and mitigation controls as required to meet safety criteria established for the protection of the public and workers. The PHA team includes members experienced in the engineering design and operation of the chemical process being evaluated and at least one member knowledgeable in the specific PHA methodology being used. The results of the PHA are also strengthened by the use of the operational and maintenance experience of the team members to compliment the design process. Specifically, the goals of PHA are to

1) Identify hazards and potential hazardous situations associated with a process or activity
2) Identify features in the design or operation of the facility that could lead to accidents
3) Assist designers in identifying the need for design features to eliminate or control hazards and hazardous situations
4) Identify principal operability concerns to assist designers in eliminating or minimizing the associated risk

The focus of the analysis is on process safety issues, such as the acute effects of unplanned radiological and chemical releases on the public or workers. The PHA supplements the more traditional industrial health and safety activities that consider, for example, protection against slips or falls, use of personal protective equipment, and monitoring for employee exposures. Additional detail on the PHA is provided in ISMP Section 5.5, "Process Hazards Analysis".

1.3.5 Facility Design/Development Activities and Safety Features Identification

The PHA and the accident analyses identify the need for accident prevention and mitigation controls to satisfy the SRD Safety Criteria. There will be differences between the prevention and mitigation techniques needed during facility operation and those needed during the deactivation process. Both sets of needs are communicated to the design groups for the selection of the most effective and efficient means of achieving the required controls. In the selection of required controls, preference is given to accident prevention over mitigation and engineered features over administrative controls. Preference is also given to passive engineered features over active engineered features (ISMP Section 3.7, "Proven Engineering Practices"). Reliance on human intervention would be used only when reliance on other means of eliminating or mitigating the hazardous situation cannot be used. The features identified are maintained or changed, as needed, as the facility moves from operation to deactivation. Control of the features is discussed in more detail in ISMP Section 3.5, "Quality Assurance Program (QAP)", Section 1.3.16, "Configuration Management", and Section 5.3, "Configuration Management".

1.3.6 Accident Analysis

During the design phase, the set of potential accidents identified by the PHA is carried forward to the accident analysis to identify the need for prevention and mitigation controls required during operation or for deactivation to satisfy the SRD Safety Criteria. The Project team experience with accident analyses for similar facilities is particularly valuable in developing the models for the accident scenarios to be analyzed. Well-established methods that include factors such as the material at risk and the rate and duration of the release of hazardous material are used in the determinations of the source terms (NRC 1988; DOE 1994).

Evaluating potential accidents involves the following tasks:

1) Separating the lower-risk accidents adequately addressed by the PHA from the higher-risk accidents that warrant quantitative analysis to confirm risk acceptance guidelines are satisfied
2) Grouping the accidents based on considerations such as the location of the accident, the phenomena involved, the accident type, and the nature of the hazardous material at risk
3) Calculating the radionuclide or chemical release from the facility and the impact of the release on the facility operators whose actions are credited to maintain the public and workers radiological and chemical exposures within defined standards

1.3.7 Acceptable Level of Public Safety

During the facility design evolution, a consequence analysis is performed for each accident involving a radionuclide or chemical release. For those accidents that involve a radionuclide release, the calculated exposures are compared to the radiological exposure standards of Table 1-2 to determine the need for accident prevention or mitigation features credited for public safety. For chemical release, the projected exposure is compared to the standards of SRD Safety Criterion 2.0-2. If the radiological or chemical release standards are not satisfied, the need for engineered or administrative controls to prevent or limit the release is addressed. These features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention or mitigation of accidents. Features credited for satisfying the public radiological exposure standards of Table 1-2 and chemical release exposure standards of SRD Safety Criterion 2.0-2 are classified as Safety Design Class (which is a subset of Important-to-Safety as discussed in Section 1.3.10, "Classification of Structures, Systems, and Components). The location of the public (i.e., offsite receptor) for the purpose of establishing compliance with Table 1-2 and the chemical release standard, is established at the most limiting exposure location along the near exposure bank of the Columbia River, Highway 240, and a southern boundary as shown in Figure 1-2. If credit is taken for operator action to satisfy the public radiological exposure standards of Table 1-2, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem TEDE whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy public chemical exposure to the standards specified in SRD Safety Criterion 2.0-2, provisions are made so that the operator exposure does not exceed the standard specified in SRD Safety Criterion 4.3-7.

Table 1-2 Radiological Exposure Standards Above Normal Background (Sheet 1)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Normal Events: Events that occur regularly in the course of facility operation (e.g., normal facility operations); including routine and preventative maintenance activities.	>0.1	Normal modes of operating facility systems should provide adequate protection of health and safety.	5 rem/yr 50 rem/yr any organ, skin, or extremity 15 rem/yr lens of eye 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b) (1)	5 rem/yr 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b) (1)	10 mrem/yr (airborne pathway) 100 mrem/yr (all sources) 100 mrem/yr (public in the controlled area) 25 mrem/yr (radioactive waste)
Anticipated Events: Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	10^{-2}<f10^{-1}	The facility should be capable of returning to operation without extensive corrective action or repair.	5 rem/event (2, 3) 1.0 rem/event design action threshold (4)	5 rem/event (2, 3) 1.0 rem/event design action threshold (4)	100 mrem/event (3)

Table 1-2 Radiological Exposure Standards Above Normal Background (Sheet 2)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Unlikely Events: Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	10^{-4}<f10^{-2}	The facility should be capable of re-turning to operation following poten-tially extensive corrective action or repair, as necessary.	25 rem/event (2, 3)	25 rem/event (2, 3)	5 rem/event (3)
Extremely Unlikely Events: Events that are not expected to occur during the life of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.	10^{-6}<f10^{-4}	Facility damage may preclude returning to operation.	25 rem/event (2, 3)	25 rem/event (2, 3)	25 rem/event 5 rem/event target (3) 300 rem/event to thyroid
Location of Receptor			Within the Controlled Area Boundary	The most limiting location at or beyond the Controlled Area Boundary	The most limiting location along the near river bank/Hwy 240/ southern boundary

(1) In addition to meeting the listed design objective of 10 CFR 835.1002(b), the inhalation of radioactive material by workers and collocated workers under normal conditions is kept ALARA through the control of airborne radioactivity as described in 10 CFR 835.1002(c).

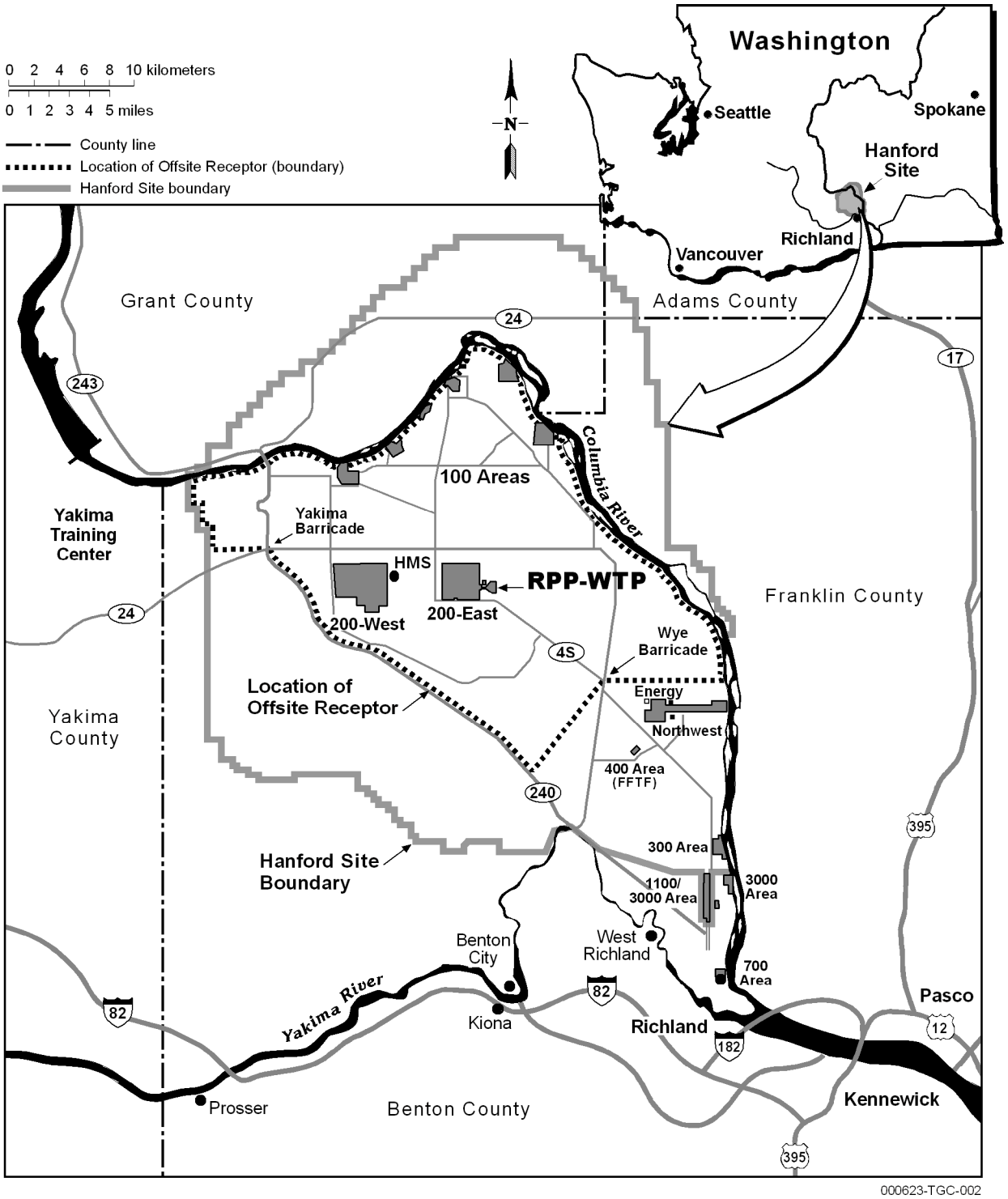
(2) In addition to meeting the listed worker and collocated worker exposure standards for accidents, the Worker Accident Risk Goal is satisfied through the calculation of the risk from accidents with accident prevention and mitigation features added as necessary to meet the goal.

(3) In addition to meeting the listed exposure standards for accidents, the Project approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below standards to account for uncertainties in the analysis and to provide for sufficient design margin and operational flexibility.

(4) When a calculated accident exposure exceeds this threshold, appropriate actions are taken. These include carrying out a less bounding (i.e., more realistic) evaluation to show that the accident consequences will be below the threshold or evaluating additional safeguards for cost effectiveness and/or feasibility. This threshold is not a limit; it does not require the implementation of additional preventative or mitigative features if they are not both cost effective and feasible.

A conservative approach is applied to accident consequence analysis in terms of input assumptions, boundary conditions, modeling techniques, and compliance with public radiological and chemical release standards. As the process and facility design mature, the analysis is refined to eliminate unnecessary conservatism that may have been applied solely to cover uncertainties in design. This strategy is consistent with a risk-based approach that allows the use of uncertainty analysis to better identify the impact of the assumptions and state of knowledge on results from the safety analysis.

Figure 1-2 Location of Public Receptor



1.3.8 Acceptable Level of Worker Safety

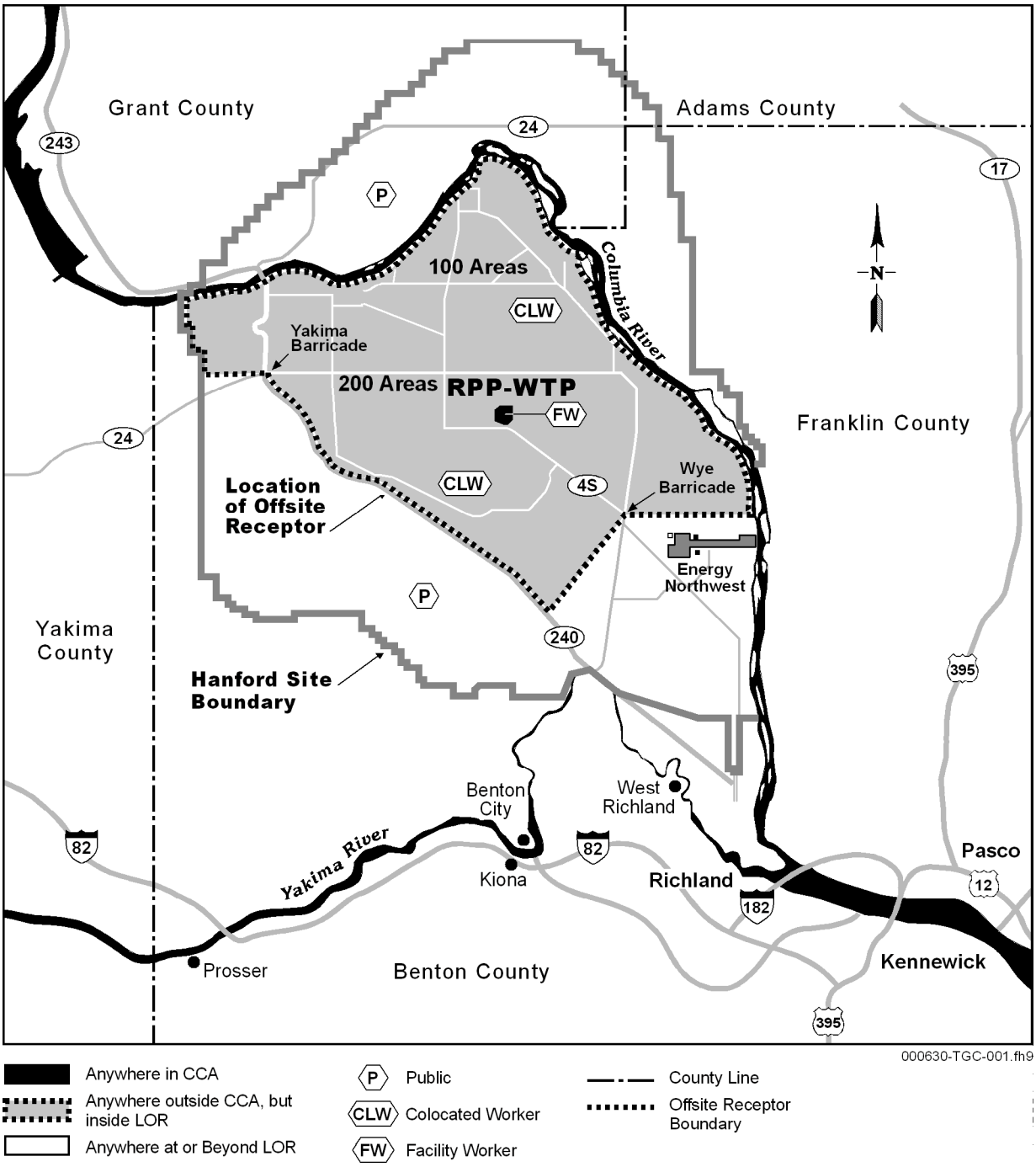
Radiological exposure standards applied to the facility worker and collocated worker are provided in Table 1-2. The location of the workers is shown in Figure 1-3. A 5 rem/event standard is applied to the workers for anticipated events, and a 25 rem/event exposure standard is applied to workers for unlikely and extremely unlikely events. The 25 rem/event standard corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2×10^{-2}. For unlikely events (defined in Table 1-2 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of about 2×10^{-4}/yr, which is less than the average of the accidental death risk for workers in some of the safest industries, such as retail and wholesale trade, manufacturing, and service (EPA 1991).

Compliance with the 25 rem/event worker standard is established using qualitative methods of the PHA supported, where necessary, by numerical analyses that may include the development of event trees and fault trees or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls to be added to the design are identified. The PHA identifies hazards and operability problems based on the design detail available and experience with similar facilities. Further hazard evaluation takes place in parallel with design development to ensure that safety is built into the design process. Having generated the list of hazards, this list is subject to a further systematic team-based review where a binning process takes place. The binning process is essentially the risk-based categorization of hazards and hazardous situations according to a frequency/consequence matrix.

The 25 rem/event worker standard for unlikely or extremely unlikely events applies to events with frequencies less than 10^{-2}/yr. For those frequencies, the PHA assigns serious and major hazardous situations as either undesirable, acceptable with controls, or acceptable. For a hazardous situation to be acceptable, the situation must have consequences less than 25 rem. Where there is uncertainty concerning the appropriate hazard category to be assigned, the hazard is binned to the higher category to ensure that the accident analysis remains conservative.

For those accidents that involve a radionuclide release, the calculated exposures are compared to the radiological exposure standards of Table 1-2 to determine the need for accident prevention or mitigation features credited for worker safety. For chemical release, the projected exposure is compared to the standards in ERPG-2. If the analysis of radiological or chemical exposures do not confirm the adequacy safety, the need for engineered or administrative controls to prevent or limit the release is addressed. These features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention or mitigation of accidents. Features credited for satisfying the radiological exposure standards of Table 1-2 and chemical release exposure standards of ERPG-2 (AIHA 1988) are classified as Safety Design Class.

Figure 1-3 Location of Facility and Collocated Workers



The worker accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to workers in the vicinity of the Contractor's facility, of fatality from radiological exposure that might result from an accident should not be a significant contribution to the overall occupation risk of fatality to workers" (DOE-RL 1996b, Section 3.1.3). This goal is satisfied by calculating the risk of facility operation to the workers at the RPP-WTP. This is a best-estimate analysis based on realistic input and modeling assumptions. In performing this analysis, all SSCs capable of preventing or mitigating the event are considered. The evaluation of the availability and reliability of the SSCs include factors such as failures to start and failures to operate, as well as unavailability resulting from maintenance activities. Accident prevention and mitigation controls are added to the design as necessary to satisfy the worker accident risk goal.

If credit is taken for operator action to satisfy the worker radiological exposure standards of Table 1-2, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy worker chemical exposure to the standard specified in SRD Safety Criterion 2.0-2, provisions are made so that the operator exposure does not exceed the standard specified in SRD Safety Criterion 4.3-7.

Additional details on the radiological exposure standards applied to the public and workers are provided in Appendix D of 24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*, which also provides information on the basis for the assumed location of the receptors.

1.3.9 Quality Assurance Program

The quality assurance program (QAP) is an important tool in achieving the goal of the safe operation of the RPP-WTP. The QAP defines the organizational structure, functional responsibilities, levels of authority, and interfaces for those managing, performing, and assessing the work to be performed. The Project developed its quality assurance program (QAP) in compliance with the requirements of 10 CFR 830.120, "Quality Assurance Requirements", so the integration of the QAP for the TWRS-P Project began during the initial phases of the project. The QAP document for Part A has been submitted to and approved by the U.S. Department of Energy (DOE) (Sheridan 1997). The QAP document for Part B activities has been submitted to DOE; this version (BNFL 1998c) has been approved by the DOE Regulatory Unit (Gibbs 2000). BNI revised the BNFL/CHG QAP document into a Quality Assurance Manual (QAM). This QAM (BNI 2001) superceded the CHG QAP document (i.e., BNFL-5193-ISP-01, Revision 8) in its entirety.

As a result of early development of the QAP, the PHA, SRD, and HAR were developed in accordance with the requirements in the QAP. The application of the requirements of the QAP continues during design, procurement, construction, commissioning, inspections, operations, maintenance, modifications, and deactivation of the facility. Administrative processes such as training, procedure development, and configuration management are subject to the requirements of the QAP. The QAP is used by the Project team to ensure that all aspects of the integrated safety approach have been implemented for the Project.

The RPP-WTP Project QAP document (i.e., BNFL-5193-QAP-01, Revision 8) was restructured to reflect BNI QA program policy, as well as use of NQA-1-1989 (ASME 1989), QARD (DOE 2000), and DOE O 414.1A (DOE 1999), as issued in a *Quality Assurance Manual* (BNI 2001). This QAM serves as the Authorization Basis document for implementation of the Project QA program. The QAP requires periodic assessments of activities, both by management and by knowledgeable, independent personnel, as described in QAM section 18. The conduct of audits to objectively evaluate the effectiveness and proper implementation of the QAM for activities affecting quality of SSCs and surveillances of specific project activities (e.g., process controls, preparation of safety documentation, configuration and document control, and records management) to supplement the compliance audit program are also described in the QAM. The QAM also describes the process of qualifying personnel who perform assessments, audits, and surveillances, as well as documentation of results and review by management.

Performance monitoring is used to verify that the necessary programs, plans, and procedures are functioning to ensure that activities are maintained in compliance with the applicable requirements. The findings of performance monitoring are used to determine if changes are needed to ensure that the high standards of performance expected are achieved.

The QAP ensures that identified corrective actions are implemented and any follow-up actions, such as the performance of a re-audit of a deficient condition, are conducted.

Different aspects of the implementation of the QAP are discussed in the following parts of the ISMP:

1) Chapter 2.0 “Compliance with Laws and Regulations”
2) Section 3.5 “Quality Assurance Program”
3) Section 5.4 “Compliance Audits”
4) Chapter 10.0 “Assessments”

1.3.10 Classification of Structures, Systems, and Components

The design classification process used on the Project provides a consistent, project-wide approach for the classification of the RPP-WTP SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs will be revised as necessary.

The design classification system provides assurance to DOE that the defined safety functions of SSCs will perform as intended.

In this system, SSCs are designated as Important-to-Safety in accordance with the definition of this term as provided in *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b).

SSCs defined as Important-to-Safety for the RPP-WTP include the following.

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Table 1-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs are designated as Safety Design Class.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs are designated as Safety Design Significant.

The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded. However, additional items also are designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis. These latter items are identified by the results of the HAR.

Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the risk analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

SSCs identified in ISAR Section 4.8, “Controls for Prevention and Mitigation of Accidents” as Design Class I and II are Safety Design Class SSCs. SSCs provided to protect the health and safety of the public and collocated workers usually are considered to also provide adequate protection of the environment. As stated in ISAR Section 4.8, “The selection of engineered and administrative controls is based on the conceptual design of the facility. Additional or different features may be identified during Part B”. The more complete group of Important-to-Safety SSCs will be identified in Part B and provided in the Preliminary Safety Analysis Report (PSAR) as part of the Construction Authorization Request. The PSAR and the Final Safety Analysis Report also will describe SSCs that are not designated as Important-to-Safety. The descriptions of these SSCs will note that they are not classified as Important-to-Safety.

When a SSC is designated as Safety Design Class it has the following attributes:

1) Quality Level 1 (QL-1) is applied to the SSC. The QAP describes the requirements associated with QL-1.

2) For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. This requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.

3) The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event. For example, if an earthquake can produce exposures to the public or workers in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed to be DBE-resistant and designated as Seismic Category I for radiological hazards (or Seismic Category III for chemical hazards). However, DBE-resistance is not applied automatically to Safety Design Class SSCs. It is applied only when the earthquake is the initiating event, or when the earthquake could cause the initiating event. A Safety Design Class SSC that does not have a DBE mitigating function is designated as Seismic Category III.

   This natural phenomenon hazard (NPH) design philosophy is used for all severe natural phenomena events (i.e., earthquake, flood, high wind). Therefore, if a Safety Design Class SSC is needed for meeting public or worker exposure standards for a given NPH event, the NPH loads associated with that event are taken from SRD Volume II, Table 4-1, "Natural Phenomena Design Loads for Important-to-Safety SSCs with NPH Safety Functions". All other NPH loads for the Safety Design Class SSC may be taken from SRD Volume II, Table 4-2, "Natural Phenomena Design Loads for SSCs without NPH Safety Functions" in lieu of SRD Table 4-1.

4) General design requirements are applied as identified in Section 4.0 of the SRD for Safety Design Class SSCs. See SRD Safety Criterion 4.1-5 as an example.

5) Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0. For example, SRD Safety Criterion 4.4-5 provides requirements associated with Safety Design Class air treatment systems.

6) Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.

7) Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements (discussed in ISMP Section 4.2.3.4 "Technical Safety Requirements").

When a SSC is classified as Safety Design Significant it is has the following attributes.

1) Quality Level 2 (QL-2) is applied to the SSC. The QAP describes the requirements associated with QL-2.
2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event. If an earthquake can produce exposures to the public or workers in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed DBE-resistant as discussed above. The same NPH loads also are applied to a Safety Design Significant SSC if failure of the item could prevent the Safety Design Class SSC from performing its safety function required as a result of the DBE. Such an SSC is designated Seismic Category II. It should be noted, however, that DBE resistance is not automatically applied to Safety Design Significant SSCs. It is applied only when the earthquake is the initiating event, or when the earthquake could cause the initiating event. A Safety Design Significant SSC that does not have a DBE mitigating function is designated Seismic Category III.

   This NPH design philosophy is used for all severe natural phenomena events (i.e., earthquake, flood, high wind). Therefore, if a Safety Design Significant SSC is needed to meet public or worker exposure standards for a given NPH event, the NPH loads associated with that event are taken from SRD Volume II, Table 4-1, "Natural Phenomena Design Loads for Important-to-Safety SSCs with NPH Safety Functions". All other NPH loads for the Safety Design Significant SSC may be taken from SRD Volume II, Table 4-2, "Natural Phenomena Design Loads for SSCs without NPH Safety Functions" in lieu of SRD Table 4-1.
3) General and specific design requirements are applied as identified in Section 4.0 of the SRD for Safety Design Significant SSCs.
4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

1.3.11 Quality Levels

The assignment of Quality Levels (QL) is the method by which the implementation of the graded quality approach discussed in 10 CFR 830.120, "Quality Assurance Requirements" is ensured. Designation of correct quality levels helps to ensure that the appropriate quality assurance requirements are applied to specific RPP-WTP SSCs. The quality levels of the Project quality assurance approach and their applications are described in the QAP.

1.3.12 Training

Training serves an important role in the Project by ensuring that the personnel involved with the project have sufficient knowledge to safely fulfill the roles and responsibilities of their assigned tasks. Training has a direct impact on safety during design, construction, operation, and deactivation of the project by:

1) Improving technical ability
2) Enhancing personal skills
3) Increasing awareness of signs of potential hazardous situations in the workplace

4) Increasing personal awareness of the potential impact of actions taken with regard to the safety of the individual, others, and the facility
5) Establishing a safety culture that clearly assigns the responsibility for safety to the individual

During the design and construction phases of the project, the training focus is on the requirements such as design evolution, compliance with regulations and commitments, construction activities, and quality assurance.

Operator training and qualification is of specific importance in the training program. The operator training program is enhanced by the experience of the Project team at other similar facilities and by the information made available during the design phase and the commissioning program. In addition, operation of the demonstration plants provides invaluable training opportunities for the facility operators.

In recognition that different training is required for different assignments, the training plan addresses the assessment of training requirements and responsibilities and the evolution of the training plan required as the project matures. Additional information on training is provided in ISMP Section 3.15 "Training and Qualification" and Section 4.2.2, "Training and Procedures". The training plan is described in ISAR Section 3.4, "Training and Qualification".

1.3.13 Procedures

Procedures are one tool by which compliance with requirements is ensured during the design, construction, operation, and deactivation of the project. All activities that may affect safety of the public and workers are performed in accordance with step-by-step instruction provided in procedures. The range of activities covered in procedures includes, but is not limited to:

1) Design control
2) Procurement activities
3) Monitoring contractors
4) Identification and resolution of nonconforming conditions
5) Operations and maintenance
6) Emergency plan implementing procedures

There is a defined hierarchy of procedures commensurate with the philosophy used to developed the tailored levels of design classification and quality levels. For example, procedures supporting the implementation of Technical Safety Requirements that are credited for accident prevention or mitigation will have a greater safety significance than procedures supporting maintenance activities on other SSCs. Those procedures, at the highest level, are subject to increased rigor with respect to their development, review, implementation, and change. Increased rigor includes requirements for independent review and approval by qualified and experienced personnel or safety committees. Training emphasizes the importance of the hierarchy as well as the content of the procedures and the requirement to follow procedures to ensure safe and efficient activities.

One category of procedures is the operating procedures. These procedures are developed during the design and construction phase, when more detailed design information is available. The design information, test data, and design requirements are incorporated into the operating procedures. The operating procedures address normal and off-normal facility conditions, process startup and shutdown, and emergency events. The development and control of the operating procedures are summarized in ISMP Section 5.6.1, "Procedure Development", and is addressed in ISAR Section 3.9, "Procedures".

1.3.14 Commissioning

Another integral portion of the safety approach is the commitment to a thorough startup testing program. The program validates that the design, construction, hardware, programs, and personnel are ready to support the safe operation of the facility. The tests performed ensure that the equipment and facility are properly built and will operate as designed prior to transition to the operational phase. In addition, the startup testing program documents the as-built configuration and the initial operating parameters of the facility. The program serves as an opportunity to perform a final system analysis and to detect significant faults prior to facility operation. The startup testing program is also used to confirm the adequacy of training and procedures to be used for facility operation.

The method of testing used in the startup testing program can require analysis, demonstration, examination, inspection, or functional test. The selection of the appropriate test method and scope of the tests are determined using a systematic analysis and are described in ISAR Chapter 3.0, "Conduct of Operations". In general, the startup testing program is a phased program, with successful individual component testing leading to system functional and interface testing, followed by the integrated system testing. A final phase of the program, testing with design waste feed materials, must be successful completed before the facility transitions to an operational phase. Additional information is provided in ISMP Section 3.14, "Startup Testing and Operation" and Section 5.6.4, "Startup Review".

1.3.15 Operations

The Project safety approach, which began with the design phase and is followed through the construction and testing phases, is also emphasized in the operational phase by establishing a set of principles for achieving excellence in operation of the RPP-WTP. This set of principles is implemented as a Conduct of Operations program (see ISAR Section 3.11, "Operational Practices") that controls and conducts the operations of the facility. Attributes of the program include the following.

1) Operation of the facility in accordance with the Technical Safety Requirements
2) The establishment of high standards
3) The communication of those standards to the workforce
4) Provisions for the sufficient number of qualified personnel required to perform the activities necessary to meet the standards
5) Implementation of a philosophy to hold workers and managers accountable for their performance

The conduct of operations program practices are major contributors to the safety of the public and workers. The practices are summarized in the ISAR Chapter 3.0, "Conduct of Operations", and detailed guidance on the practices will be incorporated in the RPP-WTP procedures. The conduct of operations program includes shift routines and operational practices (e.g., operator inspection tours, log keeping, response to indications, and resetting protective devices), control area activities (e.g., communications and on-shift training), control of equipment status, lockouts and tagouts, independent verification, operations turnover, required reading, operations procedures, operator aid postings, equipment and piping labels, and incident investigation and reporting.

Another key element in the safety approach is the involvement of operations personnel throughout the design process and the involvement of the design personnel through turnover of the facility to the operations staff (see ISAR Section 3.10.1, "Testing Program Description"). This involvement allows operations personnel not only to provide input to the design process to develop a safe and operable facility, but also to become knowledgeable in the features and limitations of systems and components of the facility. Additionally, the development of facility control system simulators in advance of facility testing strengthens the ability and confidence in the performance of the systems and the operational interfaces. The simulators provide an important integration of the design and operating personnel during the testing in further support of a smooth transition to the operational phase of the project. This interface between the designers, the operators, and the simulators ensures the ability of the Project team to demonstrate operational readiness in advance of final testing activities of the facility.

1.3.16 Configuration Management

Configuration management is one of the fundamental principles to achieve safety. Throughout the life cycle of the RPP-WTP, configuration management is applied to all activities to ensure that programmatic objectives related to radiological, nuclear, and process safety are achieved. Work is performed and controlled to pre-approved plans and procedures that delineate responsibilities. Records that define the requirements, design, verification, and acceptance of the RPP-WTP are retained to provide an accurate record of the design including approved changes to the design. Operating organizations define operational requirements and participate in design review, procedure preparation, training, and planning activities to become familiar with the features and limitations of components included in the design of the facility. Organizations that manage or interface with subcontractors or suppliers of items, activities, or services involving configured items flow down applicable requirements to ensure that the configuration management process as defined in the *RPP-WTP Configuration Management Plan* (CM Plan) (BNI 2001f) are properly implemented.

The WTP Configuration Management Program provides direction to identify and document the physical and functional characteristics of facility structure, systems, components, and computer software applications. Its application to design, construction, commissioning, operations, and deactivation activities ensures proposed changes to these characteristics are properly developed, approved, implemented, verified, and incorporated into facility design documentation. The CM Plan is based upon ISO 10007:1995(E), *Quality Management - Guidelines for Configuration Management.*

The project formally identifies and establishes configuration baselines, systematically evaluates and dispositions changes, and records the implementation of approved changes. The Configuration Management Program establishes the policies, guidelines, and responsibilities serving to ensure that:

- The engineered configuration of the project is controlled to ensure it meets design, performance, and acceptance requirements.
- Approved configuration changes are assessed for their impact on performance and safety.
- The configuration status of the technical baseline is maintained.

Configuration management is implemented through project plans and procedures that incorporate requirements from the CM Plan and other top-level requirements documents. Records including Authorization Basis documents; engineering and other source requirements documents; design documents; identification of structures, systems, and components; and links between the design documents and the requirements documents are maintained in an electronic data management system managed by Project Document Control.

Effective implementation of configuration management and supporting processes is assessed through management self-assessments in accordance with approved project procedures. Additionally, formal audits performed by Quality Assurance to their normal auditing practices verify compliance with approved project procedures.

1.3.16.1 Configuration Management Approach

The RPP-WTP configuration management program implements a process consisting of four basic steps, as follows:

1) **Identification and documentation.** The activities comprising selection of configured items, documenting their physical and functional characteristics, and allocating unique identification characters and numbers to the configured items and their configuration documents.
2) **Change control.** The activities comprising the control of changes to a configured item after formal issue of its configuration documents.
3) **Status tracking and reporting.** Formal recording and reporting of configuration documents, and the approved changes to those documents.
4) **Configuration audit.** Examination of review, inspection, and test records to determine that a configured item conforms to its configuration documents.

Project plans and procedures fully implement the configuration management process by delineating responsibilities for organizations that manage activities and provide services related to configuration management. Implementing procedures are cited in the CM Plan (BNI 2001f).

1.3.16.2 Configured Item Identification and Documentation

Configured items are selected and documented taking into consideration at what level functional and physical characteristics can be best managed to achieve the overall WTP Project performance objectives related to radiological, nuclear, and process safety. Items identified for configuration management include structures, systems, and components; plant installed software; project interfaces; and Authorization Basis documents.

1.3.16.3 Change Control

Design configuration is controlled in accordance with approved project procedures to maintain an accurate record of the design. Changes are documented to describe the change, the reason for the change, and to identify the configured item and related documents to be changed.

Change control is a formal process comprised of change documentation, evaluation, approval, and implementation.

1.3.16.3.1 Documentation

Changes must be documented except for insignificant changes, i.e., those with no affect on safety, environmental protection, the Authorization Basis, scope, schedule, or cost. When the change control process uses separate change documents, the change documents shall have unique identification numbers for status tracking and convenient to establish links to affected or related documents in the electronic data management system.

1.3.16.3.2 Evaluation

Engineering evaluates proposed changes to identify interface or discipline subject matter impacts and to establish that a proposed change should be implemented. Factors to be considered in the evaluation include compliance of the change with regulations, the Authorization Basis, applicable codes and standards, and safety and environmental significance. Environmental, Safety, and Health monitors the impact evaluation process.

1.3.16.3.3 Approval

The approval process for changes is commensurate, in detail and approval authorities, with the approval process for the original configuration. This may include obtaining authorization from the PSC, customer, or regulators prior to implementing the change.

1.3.16.3.4 Implementation

Approved changes are implemented in accordance with WTP Project procedures identified in the CM Plan specific to the various configured item types encountered in design, procurement, construction, commissioning, operations, and deactivation activities.

1.3.16.4 Status Tracking and Reporting

Status tracking and reporting consists of recording and reporting information required to manage and administer the configuration management process and related activities. Information is recorded, links to related documents entered, and sorted for reporting in the electronic data management system managed by Project Document Control.

1.3.16.5 Configuration Audits

Configuration audit is the examination of items and documents to determine whether a configured items conforms to its configuration documents. Configuration audit typically consists of functional and physical confirmation.

Functional confirmation is accomplished by identifying the individual functional and performance requirements of a configured item and confirming through review, inspection, and test records that the requirements are achieved.

Physical confirmation is accomplished by examining the physical or as-built and tested configured item for compliance to its configuration documents. Together, the functional confirmation and the physical confirmation demonstrate that the configured item, as defined by its configuration documents, conforms to the physical and functional requirements.

1.3.16.6 Functions and Requirements Management

The Contract, *Basis of Design*, *Functional Specification*, *Operational Requirements Document*, and Authorization Basis design requirements are compiled in an Access © database, designated the Design Criteria Database (DCD). The database has full text and keyword search capabilities. This database is used by design and safety personnel to identify applicable safety functions and requirements for use in the WTP design. The database is updated by procedure each time a source document is revised.

The configuration management organization maintains the *Basis of Design* and DCD to integrate design requirements, safety standards, and operational requirements.

1.3.16.7 Training

The configuration management organization develops, maintains, and provides training on the configuration management program for the project. This training includes a description of the program, reasons why the program is used, the elements of configuration management, and how the program is implemented on the project. This training is provided to employees as part of the Safety and Quality Design Required Training.

1.3.17 Incident Investigations

The importance of the identification and correction of nonconforming conditions as part of a safety approach for the Project is recognized. To ensure that significant incidents that could adversely affect the quality, security, environment, operations, or health and safety of public and workers are brought to the attention of management, the project regulator, and the DOE Occurrence Reporting and Processing System, the ISMP requires incident investigation and reporting. The incident investigations for the Project are expanded in scope to include accidental radionuclide releases and the construction and startup testing phases of the project. Also, reporting of events of less severity than those required of process safety management are included in the program. Incidents to be reported to the regulator include, for example, events or conditions at the facility that resulted in degradation of the principal safety barriers or in a condition beyond the design basis or emergency procedures. The incident investigation process requires that serious events or conditions are addressed and resolved and that the findings of the investigation are resolved.

The investigations are conducted in accordance with the Safety Criteria in SRD Volume II, Section 7.7, “Reporting and Incident Investigation”. Additional detail on the implementing procedures are contained in ISAR Section 3.7, “Incident Investigations”.

1.3.18 Emergency Planning

An important aspect of the safety approach is to ensure the health and safety of the public and the workers during emergency situations at the RPP-WTP. This is accomplished through the development of an emergency management plan for the prompt, efficient, and effective response to emergencies in accordance with the applicable local, state, and federal regulations. The development and the implementation of the emergency management plan are enhanced by the involvement of BNI with the existing Hanford emergency management community. The emergency management plan is fully implemented before radioactive wastes or hazardous chemicals are introduced into the facility. The construction manager implements state and federal emergency preparedness requirements for hazardous situations that may arise during construction.

The scope of the emergency management plan will be determined following the final assessment of the hazards and hazardous situations to be completed during Part B. The implementing procedures will ensure compliance with the applicable requirements that are identified during the development of the emergency management plan. Additional information is included in ISMP Section 3.10, "Emergency Preparedness" and is presented in ISAR Chapter 9.0, "Emergency Management.

1.3.19 Deactivation

All of the previously discussed elements of the RPP-WTP safety approach are applied to the deactivation phase of the project.

In addition, the RPP-WTP incorporates design provisions to facilitate deactivation and final decommissioning. These provisions reduce radiation exposure to Hanford Site personnel and the public during and following deactivation and decommissioning activities and minimize the quantity of radioactive waste generated during deactivation.

A deactivation plan is prepared prior to construction of the RPP-WTP. The deactivation plan provides details on how the following activities will be accomplished to achieve a deactivated status for the facility.

1) Verification of the completion of the facility deactivation end point. (The term facility deactivation end point refers to the set of conditions that comprise the completion of facility deactivation [i.e., radiological, structural, equipment, and documentation])
2) Documentation of the regulatory status, conditions, and inventories of remaining radioactive and hazardous materials and health and safety requirements
3) Modification of the facilities, structures, support systems, and surveillance systems to provide for confinement and monitoring of the remaining contamination, radiation, and other potential hazards
4) Posting and securing of the facility
5) Removal of packaged special nuclear materials and other packaged radiological and chemical materials
6) Confirmation that security systems and procedures are adequate and in place to prevent unauthorized entry

2.0 Compliance with Laws and Regulations

General compliance with statutes that relate to radiological, nuclear, and process safety is described in this chapter. Compliance with 10 CFR 830.120 and 10 CFR 835 is discussed respectively in Section 2.2, "Compliance with 10 CFR 830.120, 'Quality Assurance Requirements' " and Section 2.3, "Compliance with 10 CFR 835, 'Occupational Radiation Protection'".

2.1 Statutory Compliance

New laws, regulations, and guidance documents are identified and reviewed for applicability to the design, construction, operation, and deactivation of the River Protection Project – Waste Treatment Plant (RPP-WTP). This review is coordinated by the Environmental, Safety, and Health (ES&H) Department and performed by the professional staffs of the ES&H, Quality Assurance (QA), Engineering, and Operations organizations (see Chapter 11). Changes to laws, regulations, and guidance documents are identified by review or survey of a number of sources, such as the following:

1) *Code of Federal Regulations*
2) *Federal Register*
3) *State of Washington Administrative Code*
4) *The Bureau of National Affairs Inc. Environmental Reporter*
5) Working contacts with the U.S. Environmental Protection Agency (EPA), the State of Washington, and other regulatory agencies
6) Trade journals
7) Corporate memberships on regulatory committees
8) Web sites of various agencies (e.g., US DOE, EPA, NRC, OSHA, and DOH) and organizations

For regulations that require the submittal of an implementation plan, the plan is submitted to the regulatory authority for acceptance on the schedule defined in the regulation. Exemption requests may be considered for specific elements of a regulation. However, until the granting of such a request, all elements of the regulation are considered applicable. Exemption requests are considered for the following reasons.

1) The requirement conflicts with the requirements of other regulations.
2) Meeting the requirement is not necessary to achieve its purpose.
3) A special situation exists that is not encountered by most other projects for which the regulation applies.
4) There is a net benefit to health and safety by not following the requirement.
5) There is other public interest in the granting of an exemption.
6) Temporary relief is appropriate while a program to meet requirements is being implemented. (This item would not be considered prior to operation of the RPP-WTP.)

Actions necessary to achieve compliance with laws and regulations are included in the configuration management program, which includes the identification of the need to document changes to the authorization basis. Changes to the authorization basis are managed in accordance with ISMP Section 3.3.3, which describes the process for evaluating changes to the facility design and administrative controls for potential impact on the authorization basis (AB), including performance of safety evaluations to determine whether prior DOE approval is required (for changes other than those to the approved QAP and RPP) and requests to amend the AB, if DOE approval is required. After issuance of the Production Operations Authorization, potential unreviewed safety questions (USQs) will be evaluated in accordance with the USQ process described in ISMP Section 3.16.4. The Preliminary Safety Analysis Report (PSAR) will provide a draft USQ plan.

A change being made to the RPP-WTP technical baseline configuration relating to areas of the site; structures, systems and components (SSCs); staffing; procedures; training; and computer software are performed, reviewed, and documented in accordance with procedures to ensure that a high level of protection is maintained for the public, workers, and environment. Additional information on the Project configuration management program is provided in Integrated Safety Management Plan (ISMP) Section 1.3.16, "Configuration Management", and Section 5.3, "Configuration Management". Details on the Project configuration management program are provided in ISAR Section 3.1, "Configuration Management".

2.2 Compliance with 10 CFR 830.120, "Quality Assurance Requirements"

The Project quality assurance program (QAP) is implemented to ensure that the design, procurement, construction, testing, inspection, operation, maintenance, and deactivation activities conform to regulatory and contractual requirements. The QAP for Part A was submitted to and approved by the U.S. Department of Energy (DOE) (BNFL 1997a, Sheridan 1997). The QAP for Part B activities has been submitted to DOE (BNFL 1998c) and was revised several times. This version (BNFL 1998c) was approved by the DOE Regulatory Unit (Gibbs 2000) in January 2000. The RPP-WTP Project QAP document was restructured to reflect BNI QA program policy, as well as use of NQA-1-1989 (ASME 1989), QARD (DOE 2000), and DOE Order 414.1A (DOE 1999). The restructured QA document was issued as the RPP-WTP Project *Quality Assurance Manual* (QAM) (BNI 2001). This QAM serves as the Authorization Basis document for implementation of the Project QA program.

The QAP for the Project meets the requirements of 10 CFR 830.120, "Quality Assurance Requirements", as presented in 24590-WTP-QAM-QA-01-001, *Quality Assurance Manual* (BNI 2001). The implementation plan required by the 10 CFR 830.120 rule detailing implementation of the QA program as well as reflecting use of NQA-1-1989 (ASME 1989), QARD (DOE 2000), and DOE Order 414.1A (DOE 1999) is provided as a stand-alone Quality Assurance Provisions Document (BNI 2001a). This document is not considered part of the RPP-WTP Authorization Basis, but is a supporting document.

Adherence to the Project QAP ensures the following:

1) Missions and objectives are effectively accomplished.
2) Products and services provide their required safety functions and meet or exceed the requirements and expectations of the Project regulator. Products and services that do not meet requirements are identified, controlled, and corrected (including identification of the cause and corrective action).
3) Hazards to workers, the public, and the environment are minimized.
4) Prospective suppliers are evaluated and selected on the basis of specified criteria.

The process by which the QAP is integrated into Project activities is discussed in ISMP Section 1.3.9, "Quality Assurance Program", and Section 3.5, "Quality Assurance Program". Updating the QAP is addressed in ISMP Section 3.3.3, "Changes to the Authorization Basis". Safety Requirements Document (SRD) Volume II, Section 7.3, "Quality Assurance Program (QAP)", provides criteria for the QAP.

2.3 Compliance with 10 CFR 835, "Occupational Radiation Protection"

Implementation of 10 CFR 835 and the radiation protection program is described in this section.

2.3.1 Implementation of 10 CFR 835

BNI will be in full compliance with the applicable sections of 10 CFR 835 as discussed in the RPP. A radiological controls program that implements the requirements of 10 CFR 835 and additional requirements specified in SRD Volume II Chapter 5.0 "Radiation Protection" is established. The program includes the following components:

1) Implementation of the as low as reasonably achievable (ALARA) design goal
2) Development of the Radiation Protection Program (RPP) and implementing procedures
3) Training of personnel to the RPP and procedures
4) Selection of qualified personnel to ensure safe work performance in radiological environments
5) Maintenance of records
6) Performance of reviews and audits
7) Implementation of a lessons-learned program
8) Respiratory protection
9) Sealed sources
10) Solid radioactive waste storage, packaging, and handling

Updating of the RPP is addressed in ISMP Section 3.3.3, "Changes to the Authorization Basis".

2.3.2 Potential Exemption Request (this section has been deleted)

2.3.3 Radiation Protection Program

Title 10 CFR 835.101, "Radiation Protection Programs", requires submittal of an RPP that includes the following components:

1) Content that is commensurate with the nature of the activities performed and that includes formal plans and measures for applying the ALARA process to occupational radiation exposure
2) Specification of existing or anticipated operational tasks intended to be within the scope of the RPP
3) A program that addresses, but is not necessarily limited to, each requirement of 10 CFR 835
4) A program that includes plans, schedules, and other measures for achieving compliance with the requirements of 10 CFR 835

The RPP is managed and controlled through the establishment of procedures developed according to the requirements of the QAP.

The sequence of activities for submittal of the RPP is provided in ISMP Chapter 9.0, "Scheduling of Safety-Related Activities". Part 835 does not provide a specific schedule for submittal of the RPP for a new facility. However, Section 835.101(j) implies that DOE must be given at least 180 days for review and approval of the RPP. The sequence of activities included in ISMP Chapter 9.0 allows for a DOE review of 180 days. DOE approval of the RPP specific to Part B design activities will be requested before these activities are initiated.

The formalization and implementation of the design-related components of the ALARA program are critical to all stages of design per 10 CFR 835.1002, "Facility Design and Modifications".

2.4 Environmental Radiation Protection Program

The Environmental Radiation Protection Program (ERPP) documents the program standards, requirements, administrative controls, responsibilities, and authorities for protecting the public health and safety and environment from radiological hazards associated with the RPP-WTP during normal operations. The ERPP addresses the following elements and additional requirements of SRD Volume II, Section 5.3, "Environmental Radiation Protection", and Section 5.3.1, "Environmental Radiological Monitoring", as appropriate:

1) Activities and areas of the site subject to the ERPP
2) Measures to be used to implement the ERPP
3) Methods to be used to monitor, report, and record compliance with the ERPP
4) Models and methods used for dose assessment including bioaccumulation and dose-conversion factors
5) As Low As Reasonably Achievable (ALARA) Program
6) Effluent and environmental monitoring
7) Groundwater protection
8) Radiological protection in the management of radioactive waste

9) Controls on the release of materials

10) Property containing residual radioactive materials

The outline for the ERPP is included in the ISAR as Appendix 5B "Environmental Radiation Protection Program Outline".

2.5 Compliance with 10 CFR 820, 'Procedural Rules for DOE Nuclear Facilities'

The Price-Anderson Amendments Act (PAAA) provides indemnification to DOE contractors, subcontractors, and suppliers who manage or conduct nuclear activities in the DOE complex. DOE issued 10 CFR 820, "Procedural Rules for DOE Activities", to implement the PAAA and an enforcement policy (Appendix A to Part 820) that sets forth the DOE strategy for ensuring contractor compliance. These documents subject DOE contractors, subcontractors, and suppliers to potential civil and criminal penalties for violations of DOE rules, regulations, and compliance orders that contain nuclear safety requirements. Proactive compliance by the contractor with the enforcement policy could result in the reduction, or possible elimination of, civil penalties for a noncompliance with a nuclear safety requirement. Rules that have been issued by DOE to implement the provisions of 10 CFR 820 include 10 CFR 830.120, "Quality Assurance Requirements", and 10 CFR 835, "Occupation Radiation Protection". A number of rules have been drafted but are not yet issued for implementation. Following issuance of a specific rule under 10 CFR 820, BNI will develop implementation plans as required by that rule. BNI will comply with the requirements of 10 CFR 820. To facilitate compliance to 10 CFR 820, including nuclear safety requirements contained within the regulation, training and procedures will be developed in Part B for the following activities:

1) Identifying, reporting, correcting, and tracking non-compliances

2) Preparation, review, and approval of implementation plans for nuclear safety requirements

3) Requesting and receiving exemptions to nuclear safety rules

4) Roles and responsibilities of the BNI and DOE staff implementing 10 CFR 820

5) Procedural rules for nuclear activities

Several ancillary procedures and systems also will be developed to implement 10 CFR 820, such as a procedure for performing audits and assessments, a procedure for performing root cause analysis, a system for trending non-compliances, and a commitment database for tracking corrective actions for identified deficiencies.

3.0 Conformance to Top-Level Safety Standards and Principles

This chapter discusses the methods used to conform to top-level safety standards and principles. The top-level standards and principles include any of the safety standards or principles established in DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b). Among the many topics covered in the following sections are defense-in-depth, quality assurance, safety culture, training and qualification of personnel, emergency preparedness and internal safety oversight. Integrated Safety Management Plan (ISMP) Section 4.1.1, "Development of the Safety Requirements Document", provides additional information on how the top-level safety standards have been addressed for the Project.

3.1 Defense-In-Depth

3.1.1 Approach to Defense-in-Depth

The BNI approach to the control of hazardous situations is by prevention and mitigation. Prevention of hazardous situations takes place either by removing the hazard or hazardous situation by design (for example, by substituting a non-hazardous chemical for a hazardous chemical) or by providing administrative and engineered controls such that the frequency of the hazardous situation is acceptably low. Mitigation of hazardous situations is accomplished by providing reliable and robust protection such that, if the hazardous situation were to occur, its consequences would be acceptably low. This reliability and robustness is achieved, in part, by the preference for passive engineered features with their inherent safety. Administrative controls for accident prevention include training and procedures related to normal operation and facility maintenance and the commitment to a strong safety culture (Section 3.4 "Safety/Quality Culture"). Engineered features that enhance accident prevention and mitigation include application of proven engineering practices (Section 3.7, "Proven Engineering Practices").

BNI uses a deterministic approach to control hazardous situations. This is accomplished in tandem with the evolving design. Early recognition of hazardous situations when the design is most flexible allows maximum use of this approach. Where hazardous situations cannot be removed by design, protection is identified to prevent or mitigate the hazardous situation. The degree of protection applied is commensurate with the consequence and frequency of the hazardous situation. Defense-in-depth means that multiple layers of protection are applied against the hazardous situation such that no one layer of protection is completely relied on to ensure safe operation of the facility. The number of layers of protection, or barriers, is dependent upon the severity (i.e., consequence) of the hazardous situation to be prevented or mitigated. The analysis to show compliance to the accident risk goals (SRD Safety Criteria 1.0-3 and 1.0-5) may identify the need not only for additional barriers to satisfy the accident risk goals, but also to achieve additional defense-in-depth. One aspect of defense in depth is that no single failure of protection will allow a hazardous situation to occur. Protection is either passive or active; passive protection features are inherent features of the design that provides protection without the need for any action (e.g., shielding).

An element of the line of defense against the occurrence of hazardous situations is training and procedures that serve to reduce the probability of operator error and facilitate prompt and proper operator response to offnormal conditions. This prompt and reliable operator response serves to reduce the challenges to preventative and mitigative engineered safety features.

While operator response is an element of defense-in-depth in achieving effective mitigation of accident conditions, in the evaluation of the consequence of accidents to the chemical and radiological exposure standards, credit is normally taken only for engineered features.

When offnormal situations occur, the protection against release of radiological and chemical materials is ensured through multiple confinement barriers. Primary confinement is the process vessels, piping, and the dedicated process vessel ventilation system (with filtration). Secondary confinement is the cell or glovebox and its ventilation system. Tertiary confinement is provided by the operating corridor outside the cell together with another dedicated ventilation system. Design features that reduce exposure are conservatively assessed to ensure adequate protection against hazardous situations.

Design features that offer defense against the potential for exposure include shielded maintenance areas (bulges), ventilation systems providing filtered release, and area radiation and airborne monitoring systems that warn personnel of changing or unsafe conditions.

The application of the requirements of the quality assurance program during design, procurement, construction, commissioning, inspections, operations, maintenance, and modifications provides assurance that the engineered and administrative controls perform as required. Surveillances of specific project activities are conducted to determine compliance of in-process activities to quality assurance program requirements. Performance monitoring is used to verify that the necessary programs, plans, and procedures are established and implemented to ensure that activities are maintained in compliance with the applicable requirements.

Emergency preparedness is the final element of the Project approach to defense-in-depth. Emergency preparedness provides assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure to the public and workers. Emergency preparedness includes emergency plan implementing procedures as administrative controls and instrumentation to detect and monitor the progression of accidents as engineered features.

Defense-in-depth is applied by specifying that protection against a hazardous situation is always a combination of engineered features and administrative controls providing prevention and mitigation. This means that excessive reliance is not placed on any one system to provide the majority of protection. Each protection system (i.e., mitigative or preventative, engineered, and administrative) provides the required degree of protection on its own. The design process bins hazardous situations according to their assessed consequences and frequency, which results in obtaining a hierarchy of hazardous situations according to their severity. The more severe the hazardous situation, the greater the level of protection specified. For hazardous situations identified as having the potential to exceed the public or worker exposure standards, certain engineered features are designated as Safety Design Class (see ISMP Section 1.3.10, "Classification of Structures, Systems, and Components"). These engineered features are subject to additional design, quality assurance, operational, and maintenance requirements adding confidence in their ability to perform their specified safety function.

An example of the application of defense-in-depth is the protection provided against entry into a melter maintenance room when the melter cell shield door is open. The first line of defense against such entry is training and procedures. The training informs personnel of the high radiation field present when the melter cell shield door is open and the procedures to be followed for entry into the melter maintenance room. Procedures are used to control entry into a melter maintenance room including the use of a personnel access door key lock. Engineered features that protect against inappropriate entry include a door interlock that inhibits entry when a high radiation field exists in the maintenance room.

Facility design germane to defense-in-depth typically includes SSCs that function as the following:

1) Barriers to contain uncontrolled hazardous material or energy release
2) Preventative systems to prevent hazardous situations and to protect barriers
3) Systems to mitigate uncontrolled hazardous material or energy release given barrier failure
4) Interlocks and controls to prevent hazardous situations
5) Indication and alarms that warn of the occurrence of hazardous situations
6) Interlocks and controls to prevent access to high radiation sources

Administrative controls are linked to the overall safety management programs that directly control operation. Administrative features include the following aspect of operator interfaces:

1) Procedural restriction or limits imposed
2) Manual monitoring or critical parameters
3) Equipment support functions

In addition, risk analyses are performed to confirm that facility accident risk goals of *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006 (DOE-RL 1996b) are met. These risk analyses may show that certain events are significant contributors to the overall accident risk. Additional defense-in-depth items will be specified to reduce that risk. Conversely, if the risk assessment identifies areas of excessive conservation, unnecessary controls may be removed.

In summary, defense-in-depth is applied in the following manner:

1) Conservative identification of the hazardous situation
2) Conservatism is applied in assessing design features for normal operations such that they also provide protection against hazardous situations
3) If the hazardous situation cannot be eliminated from the design the potential consequence of the hazardous situation is conservatively assessed. This can be qualitative assessment (use of a binning matrix and judgement) or a quantitative frequency and consequence calculations if deemed appropriate

4) Use of operator training and procedures as an element of defense-in-depth (i.e., the operator responds appropriately to the development of a hazardous situation to return the facility to normal operation or to place the facility in a safe state)
5) The combination of engineered features and administrative controls provided depend on the overall severity class of the hazardous situation
6) If the potential for exceeding the public or worker radiological or chemical exposures standards exists, Safety Design Class engineered features are specified
7) Application of the quality assurance program to design, procurement, construction, and operation to provide additional assurance that administrative and engineered controls are effective
8) Emergency preparedness to provide assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure to the public and workers

Implementation of defense-in-depth for the Project is accomplished by the *Implementing Standard for Defense In Depth*.

3.2 Safety Responsibilities

BNI recognizes its corporate responsibility for safety during the design, construction, and commissioning (DC&C) phase of the project. Safety responsibilities are assigned to and by the Project Manager. The DC&C responsibilities are assigned to functional areas as shown in ISMP Tables 9-1 through 9-3. The roles assigned to organizations are provided in ISMP Chapter 11.0, "Organization Roles, Responsibilities, and Authorities". By these assignments, facility safety becomes a facility-wide responsibility with safety responsibilities identified for each functional area.

In addition, by these assignments, assurance is provided that the roles identified in the Safety Analysis Reports are carried out.

The Facility design is based on the design and operational experience gained at other nuclear and chemical facilities. As such, the potential hazards are well understood and lessons learned from earlier facilities are applied.

Part of the preparatory work for hazard identification studies is to review safety and incident reports from similar operating facilities to ensure that credible events are considered at an early stage in the design. For the RPP-WTP, the operating histories of Sellafield's Vitrification Plants, Site Ion Exchange Plant, the Enhanced Actinide Removal Plant, the Savannah River Project, and the Hanford Site plants are reviewed to take account of their operating experience. In this way, lessons learned are incorporated into the RPP-WTP design and plans for operation. One such example is ion exchange resin stability. An explosion occurred at the Hanford Z-Plant because of contact between an organic ion exchange resin and strong nitric acid (HRC 1976). Because the RPP-WTP uses both organic ion exchange resins and strong nitric acid within its processes, careful consideration is being given to design of ion exchange resin handling and storage for the RPP-WTP. Section 4.4.1, "Comparison to the Hazards Analysis Results of Other Facilities", of the Hazard Analysis Report (HAR) provides a discussion of the application of lessons learned at other facilities to the Facility process hazards analysis (PHA) and design.

3.3 Authorization Basis

In this section, the content, control, and update of the authorization basis are discussed. The authorization basis is the composite of information provided by a Contractor in response to radiological, nuclear, and process safety requirements that is the basis on which the DOE grants permission to perform regulated activities.

3.3.1 Content of the Authorization Basis

The authorization basis for RPP-WTP includes the documentation discussed in the following sections. This documentation includes that information submitted in connection with a request for Standards Approval, a request for Construction Authorization, or a request for Operations Authorization as described in DOE/RL-96-0003, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, and any other information submitted by BNI in connection with these requests (DOE-RL 1996a). Amendments to this information may be in the form of revisions to the previously submitted documents, or new information that supplements previously submitted information. The authorization basis begins at the Standards Approval regulatory action and continues throughout the design, constructions, operation, and deactivation of the RPP-WTP. The following Sections 3.3.1.1 through 3.3.1.8 delineate the elements of the authorization basis.

3.3.1.1 Integrated Safety Management Plan

The ISMP defines the process by which applicable laws, regulations, and standards are incorporated into design, procedures, and training to ensure adequate safety of the public, workers, and the environment. Further detail is provided in ISMP Section 1.1, “Introduction”.

3.3.1.2 Safety Requirements Document

The Safety Requirements Documents (SRD) defines the radiological, nuclear, and process safety objectives and standards ensuring the RPP-WTP is designed, constructed, operated, and deactivated in a manner that protects the health and safety of the public and workers and protection of the environment. These safety objectives and standards (SRD Safety Criteria), are included as a part of the RPP-WTP authorization basis to establish a formal agreement with the regulator on the necessary facility design features and management processes and the expectations on the features and processes required to safely achieve the defined work of processing Hanford tank waste. The “Radiological Exposure Standards for the Project” is included in the SRD.

Additional information on the SRD is provided in ISMP Section 4.1, “Safety Management Processes”.

3.3.1.3 Safety Analysis Reports

The Safety Analysis Reports (SAR) document the safety analysis for the facility to demonstrate that it can be safely operated, maintained, and shut down. The Initial Safety Analysis Report (ISAR) was developed during Part A based upon a conceptual design of the facility. Those portions of the ISAR that relate to the fundamental aspects of design are considered to be part of the authorization basis. The Preliminary Safety Analysis Report (PSAR) is based on the facility design and plans for construction and demonstrates adequate planning for the operational phase. The Final Safety Analysis Report (FSAR) documents the completed design and construction and provides details on the plans for operation. The FSAR includes facility and process drawings and fabrication and construction specifications important to the safety analysis of the facility. Specifications and drawings not submitted to the regulator are not part of the authorization basis. The FSAR identifies significant changes made in the facility design and plans for operation from what was presented in the PSAR. Near the end of waste processing activities, the FSAR will be expanded as necessary to discuss the RPP-WTP operating history as it affects deactivation, the hazards associated with deactivation, and the condition of the facility when it is turned over to DOE for decontamination and decommissioning.

3.3.1.4 Technical Safety Requirements (TSR)

The TSRs are based on the accident analyses included in the FSAR as related to protection of the public and workers from chemical and radiological exposures. The TSRs are maintained current so that they reflect the RPP-WTP as it is analyzed in the FSAR. It includes items in the following categories:

1) Safety limits
2) Limiting conditions for operation
3) Surveillance requirements

The limiting conditions for operation are based on the following:

1) Process variables, design features, and operating restrictions that are the initial conditions for accident analysis
2) SSCs that must function to prevent or mitigate accidents to achieve compliance to public and worker radiological and chemical exposure

The detailed content of the TSRs is prepared in accordance with Safety Criterion 9.2-3 of SRD Volume II.

The TSR Bases is a supporting document that describes the basis for the individual technical requirement (excluding administrative controls) but is not a part of the TSR.

3.3.1.5 Quality Assurance Program (QAP)

The QA Program is organized to meet the requirements of 10 CFR 830.120, principles stipulated in *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006 (DOE-RL 1996b), and the specific contract requirements for QA. The RPP-WTP Project QAP document (i.e., BNFL-5193-QAP-01, Revision 8) was restructured to reflect BNI QA program policy, as well as use of NQA-1-1989 (ASME 1989), QARD (DOE 2000), and DOE Order 414.1A (DOE 1999). The restructured QAP document was issued as the RPP-WTP Project *Quality Assurance Manual* (QAM) (BNI 2001). This QAM serves as the Authorization Basis document for implementation of the Project QA program. The QAP, as described in the QAM, provides assurance that the design, procurement, construction, testing, inspection, operation, deactivation, waste form qualification, modification, and maintenance activities conducted at the facility conform to regulatory and contractual requirements and reflect best industry practices. To support meeting project radiological, nuclear, and process safety requirements, the QAP complies with elements of NQA-1 (ASME 1989), as defined in the QAM.

The provisions of the Quality Assurance Requirements and Description document DOE/RW/0333P will be applied to QL-1 and QL-2 items and activities associated with HLW services from design through production and acceptance.

The objectives of the Project QAP are to:

a) establish the project organizational structure, management controls, functional responsibilities, levels of authority, and interfaces for managing, performing, and assessing the work; and
b) ensure confidence in the safe completion of project work in full compliance with radiological, nuclear, and process safety requirements, waste product acceptance quality requirements, and mission objectives.

Adherence to the DOE-approved QAP also ensures the following.

1) DOE mission and objectives related to Project are effectively accomplished.
2) Products and services are safe, reliable, and meet or exceed the requirements and expectations of the user.
3) Hazards to the public and workers are minimized.

The extent to which quality requirements are applied to the Project is based on a graded approach, reflecting the safety implications of the activity. Quality-related activities performed by organizations providing equipment, services, or support to the Project are conducted in accordance with the requirements documented in the approved QAP.

Additional information on the QAP is provided in ISMP Section 3.5, “Quality Assurance Program (QAP)”. Additional information on the audit and management assessment aspect of the QAP is provided in ISMP Section 5.4, “Compliance Audits”, and Chapter 10.0, “Assessments”.

3.3.1.6 Radiation Protection Program (RPP)

The occupational RPP documents the program standards, requirements, administrative controls, responsibilities, and authorities associated with the scope of RPP-WTP radiological activities. The RPP is the program required by 10 CFR 835, "Occupational Radiation Protection". The RPP provides the regulatory technical basis that ensures the radiological safety of facility workers, collocated workers, facility visitors, and the onsite members of the public. Additional information on the RPP is provided in ISMP Section 2.3, "Compliance with 10 CFR 835, Occupational Radiation Protection".

3.3.1.7 Emergency Plan

The Emergency Plan, describing the provisions for responses to operational emergencies, documents the Emergency Management Program. All aspects of the Project Emergency Management Program (EMP) as required by DOE and applicable federal, state, and local requirements are addressed. The EMP, an element of an integrated and comprehensive DOE Emergency Management System (EMS) (DOE 1995a), is designed to address emergency planning, preparedness, response, recovery, and readiness assurance activities. The DOE system considers emergency conditions that might place individuals at risk; which goes beyond radiological hazards. In addition, the relationships of the EMP to existing DOE Headquarters, DOE Richland Operations Office, and Hanford Site Contractors' programs, are documented in the Project Emergency Plan. A discussion of critical interfaces and the division of responsibility among these different agencies is included in the Emergency Plan. The elements of the Emergency Plan are designed to ensure that the Project, as part of the overall DOE EMS, is prepared to respond promptly, efficiently, and effectively to any emergency to protect the public and workers.

The Emergency Plan ensures that emergency response requirements are considered throughout the planning and design process. Emergency drills and exercises are performed to evaluate the emergency plans and RPP-WTP staff response to offnormal conditions. The exercise program includes coordination with Hanford Site, state, and local emergency response organizations. The Project will participate in Hanford Site exercises and drills for other facilities as invited.

The Emergency Plan is submitted to support the request for an operating authorization. Chapter 9.0, "Emergency Management", of the PSAR will address emergency preparedness as required to support the construction authorization request. Procedures developed by the RPP-WTP construction manager implement state and federal emergency preparedness requirements for hazardous situations that may arise during construction.

Additional information on the Emergency Plan is provided in ISMP Section 3.10, "Emergency Preparedness".

3.3.1.8 Other Information

Other documents generated by the regulator or BNI may become part of the authorization basis for the Project. This includes correspondence concerning the safety aspects of the facility design, construction, operation, and plans for deactivation. Those portions specified in Appendix E of the Part A Hazard Analysis Report (HAR) that constitute bounding or significant hazards or hazardous situations are considered to be part of the authorization basis.

3.3.2 Control of the Authorization Basis

The authorization basis for RPP-WTP is considered as an element of the technical baseline for the facility. Changes to the technical baseline are managed by a configuration management program. For further information concerning configuration management see ISMP Sections 1.3.16 and 5.3, "Configuration Management".

3.3.3 Changes to the Authorization Basis

Changes to the authorization basis include changes to the facility design and administrative controls (e.g., procedures, programs, plans, or management processes) that are described in the authorization basis or are relied on to ensure conformance to the authorization basis. Changes to the authorization basis are managed by a configuration management program discussed in ISMP Sections 1.3.16 and 5.3, "Configuration Management". As described in these sections, the change management program includes the use of qualified personnel, procedures developed and approved under the Project procedure process, and implementation under the approved QAP.

By 10 CFR 830.120(b)(3), a contractor may, at any time, make changes to the approved QAP so long as the QAP, as changed, will continue to satisfy the requirements of 10 CFR 830.120. For the Project the commitment has been made that changes that reduce commitments to a previously approved QAP, as described in the QAM, will be submitted to the DOE for review and approval per the QAM requirements for its change. Annual submittal of the QAM to DOE must also identify the changes, the pages affected, the reason for the changes, and the basis for concluding that the revised QAP continues to satisfy the requirements of 10 CFR 830.120.

As allowed by 10 CFR 835.101(I) BNI may make changes to the approved RPP so long as the change does not decrease the effectiveness of the RPP and the RPP, as changed, continues to meet the requirements of 10 CFR 835. Proposed changes that decrease the effectiveness of the RPP are not implemented without submittal to and approval by DOE. Updates to the RPP are required if a change or addition is made to the RPP. Updates of the RPP are considered approved 180 days after submittal unless rejected by the regulator.

In accordance with *DOE Position on Contractor Initiated Changes to the Authorization Basis*, RL/REG-97-13 (DOE-RL 2000), BNI may make changes to the facility or administrative controls if a review of the Authorization Basis is performed and either:

a) The review demonstrates that a proposed change is consistent with the existing Authorization Basis, or

b) The Authorization Basis is revised prior to the implementation of the proposed change.

3.3.3.1 Authorization Basis Revisions

BNI may make revisions to the authorization basis, other than to the QAP and RPP as discussed above, without prior approval of the DOE provided that the following safety evaluation and documentation requirements are met:

a. An evaluation is performed that demonstrates that the revision:

   1) Does not involve deletion or modification of a standard previously identified or established in the approved SRD.

   2) Does not involve a modification of an approved Technical Safety Requirement.

   3) Does not result in a reduction of a commitment described in the Authorization Basis.

   4) Does not result in a reduction in the effectiveness of any program, procedure, or plan described in the Authorization Basis.

   5) Does not result in an Unreviewed Safety Question (USQ), if a Production Operations Authorization has been issued.

b. A written evaluation is performed that demonstrates that the revisions to the authorization basis:

   1) Will continue to comply with all applicable laws and regulations, conform to top-level safety standards, and provide adequate safety.

   2) Will continue to conform to the original submittal requirements associated with the authorization basis document(s) affected by the revision.

   3) Will not result in inconsistencies with other commitments and descriptions contained in the authorization basis or an authorization agreement.

   The format, content, and level of detail associated with an acceptable "safety evaluation" is highly dependent on the nature of the proposed revision to the authorization basis. Rather than establishing comprehensive guidance on appropriate evaluation format, content, and level of detail, the position identifies the most fundamental basis that can applied to evaluating proposed revisions. There is a wide range of acceptable safety evaluation approaches. Also, the appropriate degree of rigor and documentation associated with the safety evaluation should be tailored to the specific authorization basis revision. The position does not indicate that an explicit and detailed case be made and documented showing that the fundamental criteria have been satisfied for all revisions to the authorization basis.

c. The following documentation requirements are met:

   1) All changes, authorization basis revisions, and associated evaluations performed in accordance with paragraphs a and b above will be documented.

   2) Documentation will be retained and readily available for DOE review.

   3) Evaluations should be documented in sufficient detail such that a knowledgeable individual reviewing the evaluation can identify the technical issues considered during the evaluation and the basis for the determinations.

   4) The DOE will be notified of revisions to the authorization basis within 30 days of completing such revision.

3.3.3.2 Authorization Basis Amendments

An authorization basis revision that does not meet the conditions of subsection 3.3.3.1 paragraph a but meets the conditions of subsection 3.3.3.1 paragraph b may be implemented following approval by the DOE of a request to amend the authorization basis. A request to amend the authorization basis includes:

1) A description of the proposed revision
2) The reason for the proposed revision
3) A descriptions of the proposed implementation schedule for the revision and associated change(s)
4) A copy of the authorization basis document or appropriate excerpt showing the proposed revision(s)
5) The safety evaluation for the proposed revision, as described in subsection 3.3.3.1 paragraphs a and b
6) If the revision involves the deletion or modification of a standard previously identified in the approved SRD, certification that the revised SRD will continue to identify a set of standards that will provide adequate safety, comply with all applicable laws and regulations, and conform to the top-level safety standards.

3.3.3.3 Decisions to Deviate from the Authorization Basis

During the design and construction phase prior to the Start of Cold-Testing, BNI may implement design changes that deviate from the Authorization Basis, provided that the provisions of paragraphs 1, 2, and 3 below are met.

1. Evaluation

   Prior to implementing a change that deviates from the Authorization Basis, BNI will perform an evaluation that determines that:

   a. The change complies with applicable laws and regulations, conforms with top-level safety standards, and satisfies the SRD Safety Criteria.

   b. The specific changes will not cause or threaten imminent danger to the workers, the public, or the environment from radiological, nuclear, or chemical hazards.

2. Documentation of Decision to Deviate from the Authorization Basis

   Documentation of BNI's decision to deviate from the Authorization Basis will be completed prior to implementing the change and will include the following:

   a. Identification of the specific changes to be implemented.

   b. Identification of the specific deviation(s) from the Authorization Basis.

   c. The evaluation described in paragraph 1.

   d. The signature of the manager(s) having the authority to approve changes that deviate from the Authorization Basis and the date such changes were approved.

   Such documentation will be readily retrievable and made available to the DOE upon request.

3. Time Limits and Notification

   a. During the construction phase, if prior approval by the DOE is required, BNI will notify the DOE (or his/her designee):

      1) either verbally or in writing within 24 hours of the decision to deviate from the Authorization Basis (as recorded in 2.d above), and

      2) in writing within 72 hours of the decision to deviate from the Authorization Basis (as recorded in paragraph 2.d above). This notification will include a copy of the documentation of the decision to deviate from the Authorization Basis described in paragraph 2 above.

   b. If prior approval by the DOE is not required, BNI will revise the Authorization Basis within 30 days following the decision to deviate from the Authorization Basis (as recorded in 2.d above) and notify the DOE within 30 days of completing such revision.

   c. If prior approval by the DOE is required, BNI will submit a request to amend the Authorization Basis to the DOE within 30 days following the decision to deviate from the Authorization Basis (as recorded in 2.d above).

   d. If provisions 3.b or 3.c are not met, or if approval of the amendment request is not obtained within 90 days of the decision to deviate from the Authorization Basis (as recorded in paragraph 2.d above):

      1) All physical work associated with implementing the change that deviates from the Authorization Basis will stop, and

      2) Corrective action will be initiated immediately, in accordance with paragraph 4 below.

4. Tracking and Resolution of Deviations from the Authorization Basis

   Changes that deviate from the Authorization Basis will be entered into the project's Corrective Action Management System (CAMS) as a condition adverse to quality, as described in the QAP. If the provisions of paragraph 3.d are invoked, the change will be recorded as a significant condition adverse to quality, and corrective action will be tracked to completion. CAMS records related to deviations from the AB will be uniquely identified to facilitate retrieval and generation of reports of the current status of such deviations upon request by the DOE.

   All revisions to the Authorization Basis associated with approved Authorization Basis deviations will be completed and all deficiencies documented under paragraph 2 will be resolved prior to Start of Cold-Testing.

3.4 Safety/Quality Culture

The BNI team understands the importance of a strong safety and quality culture in achieving excellence. To achieve a culture in which individuals involved in safety-related activities accept responsibility for the safety and quality through all phases of the Project, BNI establishes the following policy:

1) Outlining expectations and performance standards
2) Communicating those expectations
3) Implementing procedures that facilitate achieving expectations
4) Performing assessments to measure the compliance with and the appropriateness of BNI safety goals.

To achieve safety and quality throughout design, construction, and operation of the facility, BNI establishes measurable goals in the areas of industrial health and safety of workers, radiological and chemical exposure limits for the public and workers, and environmental release limits. The team then establishes policies that require the communication of the goals to employees and contractors. Communication techniques include posters, meetings, newsletters, recognition of outstanding performance, and incorporation of the goals into performance plans for groups and individuals. Another important aspect of communication is training. Employees are provided information regarding the inherent hazards of the work and tools effective in controlling the hazards or responding to hazardous situations encountered during the work processes. Managers and supervisors are expected to be familiar with the work processes and to understand the potential hazards and hazardous situations.

Other policies that establish standards of conduct and job site work rules are communicated to employees. The policies empower RPP-WTP employees to stop the activity in which they are involved if the work procedure or process is not clear or the activity appears unsafe. The policies also direct that performance reviews emphasize the requirements for safety and quality.

The safe completion of a quality job requires planning that takes into consideration aspects such as adequate work packages, appropriate level of instructions, evaluation of the impact of the task on other SSCs or processes, and an evaluation of the completed activity. Procedures governing these activities specify that trained and qualified personnel are required to participate in planning process. This includes craft and operations personnel supporting technical and administrative workers.

To ensure that safety and quality procedures are being followed and that the implemented procedures are adequate to facilitate achieving the expectations, assessments of work activities performed and the results of compliance with goals are conducted. Where practices are identified that improve safety and quality, those practices are incorporated into operations. Any required corrective actions identified are tracked to completion. Results of these assessments are provided to managers and workers.

As the project moves through design and operations to deactivation, the BNI team revises the goals and procedures to reflect the activities required for each phase.

3.5 Quality Assurance Program (QAP)

The Project QAP for all activities meets the criteria of 10 CFR 830.120, "Quality Assurance Requirements". Implementation of 10 CFR 830.120 is addressed in ISMP Section 2.2, "Compliance with 10 CFR 830.120, "Quality Assurance Requirements".

Integration of the QAP into the Project safety approach began with the PHA, SRD, and HAR developed by specific procedures in accordance with the requirements of the QAP. This included the establishment of personnel training and qualification requirements, confirmation that personnel met the training and qualification requirements, application of technical review, and documentation of results. The performance of the accident analysis and the comparison of the results of the analysis to the radiological and chemical exposure standards is also performed in accordance with the requirements of the QAP. This includes training and qualification requirements; computer code verification; independent review of input assumptions, analytical methods, and calculations; maintenance of a calculation log; and documentation of the results.

The application of the QAP to design, procurement, construction, testing, inspection, modification, and maintenance of SSCs credited with public and worker safety is discussed in the QAP. The manner in which requirements of the QAP are imposed on subcontractors is discussed in ISMP Section 5.2, "Control of Subcontractors".

Personnel training and qualification and procedure development credited for public and worker safety during facility operation are developed in accordance with the requirements of the QAP. The QAP is applied to the Emergency Management Program in the areas of training and qualification of emergency response team members, assessment of the program effectiveness, and records documentation. Additional details on these aspects of the emergency response program are provided in ISAR Chapter 9.0, "Emergency Management".

Project compliance with DOE/RW-0333P*, Quality Assurance Requirements and Descriptions for the Civilian Radioactive Waste Management Program (QARD)* (DOE 1995b) is addressed in ISMP Section 3.3.1.5 "Quality Assurance Program (QAP)". The provisions of the Quality Assurance Requirements and Description document DOE/RW/0333P will be applied as described in the QAP.

ISMP Section 5.3, "Configuration Management", Section 5.4, "Compliance Audits", and Section 8.0, "Document Control and Maintenance" provide additional information on the application of the QAP to the Project safety approach.

3.6 Facility Design for Postulated Events

This section describes the facility design for normal operation, anticipated operational occurrences, and accident conditions.

3.6.1 Normal Operations

The facility design provides for control of radiological exposure to the public and worker such that the exposures are within the standards provided in Table 1-2 for normal events. In addition, the design satisfies the Operations Risk Goal of *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006 (DOE-RL 1996b) and of SRD Volume II, Safety Criterion 1.0-4. Those SSCs required for achieving compliance with the public and worker exposure standards for normal operation are designated as Important-to-Safety Safety Design Significant as discussed in ISMP Section 1.3.10, "Classification of Structures, Systems, and Components".

The process follows a logical approach, beginning with defining the basis of design and developing the overall process flowsheet. System-specific flow diagrams, such as ventilation flow diagrams, are also developed if required. The next stage is the production of operation and maintenance philosophy documents for each area of the facility, tied together by an overall control philosophy document. These documents define the design principles for each area and allow specific equipment selection or design to commence. These principles are based on existing successful operation of structures, systems, and components. However, where a new process or system that has the potential to provide a cost-effective and safe alternative is identified, a research and development program is initiated to support the design process.

Flow diagrams and documents are subject to review during their development, addressing different aspects of the design. The Technical Organization ensures a consistent design approach is taken across the project and that all of the project requirements are being addressed. The PHA team, which includes representatives from operations, reliability, and relevant technical disciplines, addresses each component of the design from a safety and operability aspect.

This process is used at the RPP-WTP to ensure that safe, efficient operation is built in at the design stage. Application of this process is demonstrated in various philosophy documents and plant layouts that describe features to be used in the RPP-WTP. The following is a list of these features:

1) Fluidic devices (pumps and valves) that contain no moving parts are used to transport and divert highly radioactive liquids. These items require no maintenance
2) Fully welded pipework systems minimize the risk of leakage
3) Automated sampling and transport systems allow efficient process operations while minimizing radiation exposure to workers
4) Canister HEPA (high efficiency particulate air) filters ease handling and installation operations.

The type of control identified through the design process for the RPP-WTP also leads to the reduction of the risk to public and workers while allowing efficient process operation. The distributed control system allows the facility to be operated under normal conditions from a central control room, thus reducing radiological exposure to personnel. Hardwired backup systems are used for some safety systems that are totally independent from the operational control system.

The close relationship between Hanford tank farms operations and the RPP-WTP may require additional administrative controls and documentation in support of AP-106 operations (e.g., master pump shutdown). Such concerns are addressed and resolved at a site-wide level through interface control meetings.

3.6.2 Anticipated Operational Occurrences

The RPP-WTP will have anticipated operational occurrences that are not considered part of the normal process operation. Certain features are built into the design to minimize the risk to personnel, the impact to the process operation, and to enable equipment to be maintained in a safe manner during normal operation and anticipated operational occurrence. Examples of these features include the following:

1) Flasking systems that allow maintainable plant items to be removed from the cell environment and taken to specifically designed maintenance areas
2) Cell bulge systems that enable equipment to be safely maintained without needing to enter the high radiation level cell confinement
3) Standby filtration systems that allows filters to be changed offline
4) Distributed control system that contains a dedicated mode that is interlocked to prevent the maintenance of an item until it is fully isolated.

3.6.3 Accidents

During postulated accidents, the RPP-WTP is designed to maintain confinement of radioactive materials, thus preventing a significant release from the facility.

During facility design evolution, hazardous situations identified by the PHA and the accident consequence analysis are compared to the radiological and chemical exposure standards provided in SRD Safety Criteria 2.0-1 and 2.0-2. Hazardous situations considered include both internal and external events. If the radiological or chemical exposure standards are not satisfied, the need for engineered or administrative controls to prevent or limit the release is addressed. Preference is given to engineered features over administrative controls.

Hazardous situations considered include both internal and external events. The HAR Section 5.0, “Hazard Evaluation by Process Step”, discusses the internal events and HAR Section 2.1, “Site Description”, discusses external events. The ISAR Chapter 4.0, “Integrated Safety Analysis”, presents additional consideration given to internal and external events.

The engineered features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention and mitigation of accidents. Recognized and accepted consensus codes and standards are used. Features credited for satisfying the public and worker radiological and chemical exposure standards of SRD Safety Criteria 2.0-1 and 2.0-2 are classified as Safety Design Class. Details on the classification process and the quality assurance provisions provided for each classification are provided in ISMP Section 1.3.10, “Classification of Structures, Systems, and Components”, and Section 1.3.11, “Quality Levels”. Additional information on the design of SSCs credited for worker and public protection is provided in ISMP Sections 3.1, “Defense-in-Depth”, 3.7, “Proven Engineering Practices”, and 3.11, “Safety Systems Design”.

A specific list of SSCs credited for worker and public protection is provided in ISAR Section 4.8, "Controls for the Prevention and Mitigation of Accidents". These SSCs are identified in the master equipment list, which is maintained by the Configuration Management Program as discussed in ISMP Section 5.3, "Configuration Management".

3.7 Proven Engineering Practices

The RPP-WTP design incorporates the use of proven technologies so that lessons learned from the use of the technology is incorporated into the operation of the facility. For the novel uses of existing technologies (such as the use of specific ion exchange resins), the PHA ensures that the safety aspects are examined in a structured research and development program to be assured that hazard potentials are reduced as far as practicable or that protection put in place is commensurate with the assessed magnitude of the hazard.

Facility processes are based on selected technologies that minimize the risk of radiological and chemical exposure. For example, sampling and maintenance activities do not require breach of confinement; hands-on maintainable items within active areas are accessible via shielded access areas that have decontamination facilities installed; and samples with high activity levels are dispensed and transported remotely.

New and novel uses of existing technologies and processes are employed to enhance the process while maintaining safe operation. These uses (e.g., selection of ion exchange resins and the melter feed processes) are examined through a program of research and development. Such development work includes operating a pilot (cold operation) melter and associated feed and mechanical handling systems. This prototype is used to examine and prove novel processes, test the design and maintainability of components, and provide operator training in operational and maintenance activities. To support the use of new and novel uses of existing technologies and processes and new equipment, it may be necessary to develop ad hoc standards. The use of ad hoc standards is discussed in SRD Volume I, Section 3.4.2, "Identification of Consensus Codes and Standards".

The RPP-WTP design incorporates passive and active engineered features that prevent and mitigate the potential for radiological and chemical exposures to the public, worker, and the environment. In the selection of required controls, preference is given to accident prevention over mitigation and engineered features over administrative controls. Preference is also given to passive engineered features over active engineered features. The designation of safety features is made during the hazard evaluation and accident analysis processes.

Examples of passive and active features are described in the following sections.

3.7.1 Passive Features

Facility processes are confined by at least two barriers. Facility and process equipment provides the first barrier and a cell or similar enclosure provides the second. This secondary confinement barrier has appropriate levels of shielding to ensure that radiological exposure does not exceed standards. Confinement and shielding design are established, as are the codes and standards that are used. Aspects of confinement design ensure that failure of one barrier does not lead to failure of the other (i.e., confinement is diverse). For example, should a process vessel or pipework leak (loss of primary confinement), the liquor drains to the cell sump where it can be recovered. The cell is lined to prevent liquor leakage. The potential for failure of a process vessel or piping is reduced by the selection materials resistant to erosion and corrosion and the use of direct inspection or erosion/corrosion coupons as discussed in Section 3.13, "Reliability, Availability, Maintainability, and Inspectability (RAMI)".

3.7.2 Active Features

The facility ventilation systems are designed to minimize the potential for radiological and chemical release into or out of the facility. The air flow into the facility is drawn through areas designated as having low or no potential for radiological or chemical release, through areas of successively higher potential. Except for the facility ventilation systems serving areas evaluated as having marginal potential for radiological contamination, this air is then filtered before release. Ventilation systems are exhausted to the atmosphere via monitored stacks. The principles behind the design and the systems employed are tried and tested components. Additionally, important to safety ventilation systems contain redundant equipment (fans, filters, electrical supply) to protect against single active failures.

The selection of facility equipment required to perform a safety function is based on proven design. The safety performance function requires that suitable testing and maintenance regimes are in place to ensure reliability. For example, where programmable logic controllers are used, specific attention is given to their unique requirements relative to software verification and protection against electromagnetic interference (See SRD Safety Criterion 4.3-1).

Protection systems are an integral part of defense-in-depth as described in ISMP Section 3.1, "Defense-in-Depth".

Preference is given in the facility design to components failing in their safe position on loss of motive power. During the design process, the failure modes of safety features are determined and specified. Simple and proven items of equipment (e.g., valves and pumps) are used, the (required) failure modes of which are well understood and categorized.

3.8 Criticality Safety

A criticality event within a nuclear chemical facility can have severe consequences; therefore, the preferred approach is to preclude the possibility of the hazard by the use of design features. Where this cannot be achieved (because of the presence of a large mass of fissile material within the process) or is impracticable, stringent criticality controls are required. Handling large amounts of fissile material (as in plutonium finishing), criticality control is achieved through a combination of geometry, inventory control, concentration (for solutions), moderation, and suitable instrumentation backed up by administrative controls. The need for these controls is established during the design phase by considering worst-case scenarios and applying conservative assumptions. Worst-case scenarios are modeled using validated computer codes to determine system reactivities and the degree of criticality control required.

The modeling and worst-case scenarios include considerations for uncertainties in the data and calculation methods, uncertainties in the immediate environment under accident conditions, and the presence of water moderation and reflections unless the presence of water is shown to not be credible. The analysis will show that the multiplication factor, k_{eff}, will not exceed 0.95 at a 95% confidence level for credible normal, off-normal, and accident conditions. Exceeding a multiplication factor of 0.95 is prevented by either the control of two independent process parameters, or a system of multiple controls on a single process parameter. This is application of the double contingency principle.

This methodology has also been applied to the RPP-WTP process. The amount of fissile material present in the contract feed has been conservatively estimated, then modeled under process conditions using conservative assumptions. The application of this methodology indicates there is insufficient concentration of fissile material to give rise to a significant potential for criticality within the RPP-WTP. The results of this preliminary analysis are provided in ISAR Chapter 6.0, “Nuclear Criticality Safety”. If any significant potential for criticality becomes apparent, appropriate controls will be implemented commensurate with the assessed potential. Additional detail regarding criticality prevention are provided in ISAR Chapter 6.0, “Nuclear Criticality Safety”.

The RPP-WTP criticality program includes the following:

1) Establishment and maintenance of controls needed to ensure that material specification for proposed feed to the facility are fully compatible with the process and are within the fissile material content bounds of the criticality assessments
2) Performance of nuclear criticality safety assessments when and where appropriate to ensure that changes do not occur that impact assumptions made in criticality evaluations
3) Maintaining appropriate access to trained nuclear criticality experts.

The need for criticality alarms is determined by evaluation to the requirements of Safety Criterion 3.3-6 of SRD Volume II. Alarms, if required by this criterion, are installed in accordance with Safety Criteria 3.3-7 and 3.3-8.

3.9 Radiation Protection Practices

The radiation protection design practice for normal operations at the Project consist of two main elements, radiation protection design and as low as is reasonably achievable (ALARA) design. These design practices ensure that the RPP-WTP can be operated in a manner that maintains normal occupational exposures and emissions of radioactive effluents within limits and ALARA. The radiation design process also considers features to facilitate deactivation and decommissioning of the facility and will be applied to the deactivation planning near the end of waste processing operations.

3.9.1 Radiation Protection Design

Radiation protection design addresses material confinement, shielding and access control features, and monitoring. Each of these is addressed in the following sections.

3.9.1.1 Radioactive Material Confinement

Confinement systems present barriers to the uncontrolled release of radioactive material and against the spread of contamination through the RPP-WTP. For the facility, the process vessels and piping and the process vessel ventilation system provide the primary confinement barrier. The process cell structures and associated ventilation system provide the secondary confinement barrier. The operating area structures and associated ventilation systems provide a tertiary confinement barrier. Ventilation flow is from areas of lower potential contamination to areas of higher potential contamination. The effluents are treated as necessary to control exposures to collocated workers and members of the public during normal operations and under accident conditions.

Throughout the RPP-WTP confinement barrier, boundaries are identified and design criteria established for these boundaries and for the associated ventilation systems. Design documents covering the confinement systems are reviewed to ensure the design criteria are adequately implemented.

The confinement systems under normal operations are assessed based on upper-bound conditions identified in the PHA. The projected annual radiological exposure from normal operations is compared against the criteria provided in SRD Volume II, Chapter 2.0, “Radiological and Process Standards”, and facility features are modified and added to the facility as necessary to meet the criteria (BNFL 1997d).

3.9.1.2 Radiation Shielding and Access Control Features

The RPP-WTP is divided into radiation zones. The zoning reflects the intensity of the radiation sources in the area, if any, and the anticipated personnel access requirements. Maximum allowable exposure rates in accessible areas are defined to ensure that personnel exposure standards are not exceeded. Shielding requirements are then established as necessary to ensure that the exposure rates in the radiation zones are maintained under all anticipated operating conditions and that commitments to ALARA are satisfied. Shielding and access control features are provided in accordance with 10 CFR 835 and additional criteria provided in SRD Volume II, Chapter 2.0, “Radiological and Process Standards”, and Chapter 5.0 “Radiation Protection” (BNFL 1997d).

Radiation protection features such as facility zoning, minimum shielding requirements, and access control features will be documented on applicable facility layout drawings and other design documents. These documents are reviewed to ensure that the requirements are met. Details, such as penetrations are analyzed to ensure that potential streaming paths are identified and properly shielded.

3.9.1.3 Radiation Monitoring

Fixed area radiation monitoring is provided in areas where the area exposure rates may change suddenly. These sudden changes may be a result of process operation or maintenance activities. Continuous air monitors are provided in accessible locations where concentrations of airborne radionuclides may vary. Air sampling capability is also provided. Effluent sampling is provided as necessary to demonstrate compliance with regulations. The radiation monitoring locations will be shown on drawings developed during detailed design.

3.9.2 ALARA Design

Project procedures are established to implement an ALARA program. These procedures include guidance on ALARA design considerations appropriate to the facility and delineate the ALARA design responsibilities of individuals on the project. The ALARA guidance is derived from federal and commercial nuclear operating experience as well as from industry standards such as NRC Regulatory Guide 8.8, *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations will be As Low as is Reasonably Achievable* (NRC 1978) and DOE G 441.1-2, *Occupational ALARA Program Guide*. The ALARA guidance addresses considerations for reducing exposures within the RPP-WTP from operations and from final decommissioning activities. It also addresses considerations for reducing effluents from the RPP-WTP.

ALARA design criteria and ALARA design considerations are provided to project staff in controlled documents. These criteria and considerations are arranged by topic area (for example, General Criteria, Dose Criteria, Environmental Criteria, Facility Arrangement Considerations, Shielding Considerations, System Design Considerations, etc.). Design engineers are responsible for implementing and documenting ALARA design criteria and ALARA design considerations in their work. Supervisors are responsible for ensuring that individuals in the group are trained in ALARA criteria and considerations, and for reviewing designs against those criteria and consideration. The WTP ALARA program also requires an ALARA review of proposed changes to the facility.

Periodic interdisciplinary project ALARA reviews are conducted to ensure that ALARA concepts are being integrated into the design and to discuss implementation of the ALARA design goal and the rationale for exceptions from specific ALARA design considerations.

In addition, collective exposure estimates assess projected exposures to provide insight into the sources of exposure and indicate areas that may require additional attention. The estimates are compared to those from similar operating facilities.

Radioactive systems at the RPP-WTP are designed to minimize the potential for leaks of radioactive material. Radioactive leaks are collected and segregated from non-radioactive waste streams. To the extent possible, radioactive leaks are returned to the process stream.

Melter offgas streams are treated to scrub out radioactive particulates before passing through filter media. The scrub streams are returned to the process stream.

The interfaces between non-radioactive service systems (e.g., cooling water) and radioactive systems are designed so that any leakage is from the clean side to the radioactive side of the interface.

The confinement system design and access control features described above serve to minimize the spread of radioactive contamination in the RPP-WTP. During operation, movement of clean materials into potentially contaminated areas is minimized to aid in contamination control, minimize replacement and survey costs, and minimize radioactive waste volumes and costs. Tools in contaminated areas are controlled and reused to the extent possible.

3.10 Emergency Preparedness

The Project implements and maintains an emergency management program to respond promptly, efficiently, and effectively to emergencies involving RPP-WTP, activities, or operations. The applicable requirements of federal, state, and local agencies are integrated into a single comprehensive program. The magnitude and scope of the emergency management program are determined by the final assessment of the hazards and hazardous situations to be completed in Part B.

The Project emergency management program is being designed to function within the existing Hanford emergency management community. Community planning partners are the DOE; DOE contractors; the Energy Northwest; U.S. Ecology; the State of Washington; and Benton, Franklin, and Grant Counties. The Project emergency management program is being developed and will be implemented to be consistent with the *Hanford Emergency Response Plan* (DOE-RL 1994), to ensure a timely and integrated response and to eliminate duplication of effort within the planning community. Agreements will be established to enable the Project to use existing Hanford response capabilities (e.g., fire, medical, hazardous materials spill response, consequence assessment, law enforcement, and communications). The facility design facilitates access and intervention by the Hanford Site fire department (e.g., the ability to connect to the interior standpipe system). The RPP-WTP Emergency Management Administrator participates in and supports Hanford Site and local area emergency planning organizations, including the Hanford Emergency Planning Council and the local Emergency Planning Committee.

The Project emergency management program is being developed for compliance with the requirements of 40 CFR 355, “Emergency Planning and Notification”, 29 CFR 1910.38, “Employee Emergency Plans and Fire Prevention Plans”, and WAC 173-303-350, “Contingency plan and emergency procedures”.

The Emergency Response Plan incorporates into one document an overview of the emergency management program for the Project. The plan provides a description of how the Project implements the provisions of all applicable requirements. RPP-WTP specific emergency implementing procedures are developed to implement the requirements of the plan.

Table 3-1 lists the information to be included in each section of the Emergency Response Plan. Additional information on the Project Emergency Management Plan is presented in ISAR Chapter 9.0, “Emergency Management”.

3.11 Safety Systems Design

For facilities designed and built by the RPP-WTP contractor, a proven method for identifying the requirements of operational and engineered protective measures is undertaken, the results of which are applied during the entire project design phase. The RPP-WTP contractor approach to facility design applies a suite of company targets to facilitate compliance with RPP-WTP contractor standards and compliance with applicable radiological exposure standards. Where practical, passive features are used rather than active features. Potential faults are minimized by a design that moves the facility towards a safe state in response to failures, or by incorporating permanently available, passive features that render the facility safe following a failure. In some cases, however, it may be necessary to incorporate active engineered features into the design of a facility that act in response to the fault to render the facility safe.

The following hierarchy of safety measures is incorporated into the RPP-WTP design.

1) Operational Preventive Measure (OPM) is a corrective action taken by an operator to terminate the development of a fault sequence. Examples include operator responses to system parameters, sampling and chemical analyses, control system indications or alarms, and procedural instructions. An OPM is considered the first line of protection against a hazard under normal facility operating conditions. Should the OPMs fail, protective systems and devices are designed to automatically operate.
2) Engineered Protection Systems operate automatically to prevent a hazard from occurring, and generally use hardwired trips, mechanical devices, or programmable electronic systems (such as programmable logic controllers) commensurate with the potential risk of the hazardous situation. If protective measures fail, a hazardous situation may occur, the consequences of which can be reduced by the action of mitigating systems.
3) Mitigating Systems attenuate the consequence of a hazardous situation once it has occurred. They include ventilation systems, radiological alarm systems, and evacuation systems.

Table 3-1 Outline And Content of Emergency Response Plan (Sheet 1)

Section Title	Content
Introduction	The purpose and scope of the plan is presented and all requirements applicable to the Project emergency response program are identified. A description of the operational use of the Emergency Plan and Emergency Plan Implementing Procedures is provided. The types of emergencies to which the Emergency Plan applies and does not apply are identified. A description of the boundaries, facilities, and site for which the Emergency Plan applies is provided. The concept on which emergency planning is based is discussed and the documents, reports, surveys, and assessments used to develop the Emergency Plan are referenced. A summary of the results of the RPP-WTP safety analysis is given.
Emergency Response Organization	The overall organizational structure of the Project, and the emergency response organization, including its relationship to the overall structure, is described. The functions, authority, and responsibility of all internal organizational elements with emergency responsibilities are delineated. The chain of command in the event of an emergency is identified. The organizational structure, authorities and responsibilities, and roles played by each position are defined and the succession of authority for each position is identified.
Offsite Response Interfaces	An overview of the relationships with offsite organizations is provided. A description of the agreements with state, federal, and other agencies, specifying the role of the agency, potential response, regulatory control, and notification chain required is provided. Also, a list of all memoranda of agreement and memoranda of understanding with offsite organizations is included.
Emergency Categorization and Classifications	The definitions of operational emergencies, emergency classes, and the criteria used to define an emergency are stated. A brief description of the methodology used to develop criteria is given and specific technical supporting documents are identified. The Emergency Action Levels (EAL) used to define an emergency are discussed. The methodology used to develop EALs is described and reference technical supporting documents are identified. The criteria for each emergency classification are stated. Personnel (positions) responsible for declaring an emergency and their required qualifications and training are identified.
Notifications and Communications	The required and proceduralized notification process for onsite and offsite notifications for all operational emergencies is discussed. Personnel (positions) responsible for both initiating and receiving notifications are identified and the methods used to perform notification are identified. The notification procedure for termination of an incident is described. Personnel (positions) required to be notified for any emergency are identified. The circumstances under which the DOE and Hanford Site contractors are notified of an emergency are discussed and descriptions of the communications interfaces with offsite organizations are provided. Equipment, back up equipment, readiness assurance, and testing procedures are identified.
Consequence Assessment	The procedure(s) used to determine the potential consequences based on the results of hazard assessments and input from other pertinent areas are described. The methodologies used for consequence assessment and referenced technical supporting documentation are identified. The procedure for coordination with federal, state, and local organizations to obtain the information necessary to make accurate and timely consequence determinations is discussed.
Protective Actions and Recovery	The purpose and intended use of protective actions are discussed. The protective actions used at the facility and under what circumstances they are implemented, modified, or terminated, and how this information is communicated, both onsite and offsite are described. A description of the provisions for implementing protective actions at the facility and for recommending protective actions to offsite agencies is included. Conditions, procedures, and authorities for the protection of local populations are identified and the size of the plume emergency planning zone is provided. Discussion of the criteria for reentering areas under emergency conditions or reentering areas that have been access-restricted during the emergency is included. Provisions to place and maintain the facility in a safe state following an accident are discussed. Personnel (and their relationship to the emergency organization) who can develop, approve and, implement reentry are identified. A description of the system to ensure safe shutdown of operations following the declaration of an emergency is given.

Table 3-1 Outline And Content of Emergency Response Plan (Sheet 2)

Section Title	Content
Emergency Medical Support	The medical capabilities available onsite and offsite (e.g., local communities) to respond to an emergency are described. The transportation and evacuation capabilities, equipment, and the process for moving contaminated and non-contaminated casualties are described. The personnel (and their positions) with the responsibility and authority to evacuate injured or ill staff are identified.
Emergency Termination and Recovery	The plan and criteria for declaring an emergency condition terminated and for transitioning to recovery activities is described. Termination authority and responsibility, recovery criteria for protection of workers and the general public from hazardous exposure, exposure guides for recovery personnel, facility accessibility (including recognition of uninhabitable areas), security considerations, access to protective clothing and equipment, availability of medical assistance, and requirements for establishing the recovery organization are identified.
Public Information	The program to provide information and answer questions concerning the emergency to workers, media, and the general public, including information release approval, is described. The facilities and communications equipment used to disseminate information to the public are identified. The education program to inform workers and the public of the dangers present, and provide information that can be used for emergency actions, including recommended evacuation routes and sheltering is discussed.
Emergency Facilities and Equipment	All primary and back up facilities to be used for emergency response and the equipment capability and limitations, quantity of equipment, locations (both fixed and portable equipment), consumables, maintenance requirements, certification requirements, expiration dates, and computer/communications compatibilities are listed and described.
Training and Drills	The goals and objectives of the training and drills program; courses given to emergency management personnel; and identification of training requirements for key emergency management positions and response teams are provided. The periodicity of courses and employee requirement for training and retraining or refresher training are identified. Also described are the system of training available to, and required for visitors, vendors, and subcontractors; the training available to offsite organizations, and supporting organizations in order to support their abilities to participate in site emergency response actions; and the system of recordkeeping to verify training requirements are met. The drill program, including the goals, frequency, complexity, and integration of lessons learned into emergency planning is described.
Exercises	The intended purpose of the exercise program is discussed. How exercises are controlled and evaluated, and how lessons learned from exercises, improvements, and/or corrective actions, are incorporated into emergency planning is described. The varying degree to which outside agencies will participate in exercises is also discussed.
Program Administration	The Project Emergency Management Program Administrator is identified. The procedure used to control the Emergency Plan and to ensure periodic review and update; and the site internal assessment program are described. The provisions for document control and records management are provided.

Application of the design standards results in a facility in which systems operate safely, with operators monitoring the systems so that actions can be taken to terminate the development of a fault sequence. However, no credit is taken for that operator response, so the facility is designed with engineered features that will function automatically to prevent the development of hazardous situations. If system operations, operator actions, and engineered features fail to preclude the event, mitigating systems are designed to attenuate the consequences of the event.

Another important aspect in safety system design is the evaluation of the conditions in which the systems are expected to operate. The design will incorporate the expected environmental conditions into the specifications for the SSCs that must function to prevent hazardous situations or mitigate the consequences of accidents. Requirements regarding the environmental qualification of Safety Design Class systems and components, including considerations for aging, are provided in SRD Volume II as Safety Criterion 4.4-2. While suppliers of Safety Design Significant systems and components are not specifically required to provide test results relative to aging, the procurement specifications for these systems and components will specify the environmental conditions (e.g., temperature, humidity, and radiation field) to be expected during normal operation and the accident duration for which the system component must function. Specifying Safety Design Significant systems and components in this manner provides reasonable assurance to DOE that they will perform their safety function when required.

The safety system design process for the RPP-WTP uses a project-wide approach for the classification of the SSCs based on their importance to accident prevention and mitigation. This approach ensures that specifications for SSCs are commensurate with the importance of the functions that need to be performed.

Safety Design Class SSCs are those necessary to ensure that the radiation and chemical exposure standards for members of the public or workers are not exceeded as a result of accidents. The Safety Design Class designation is also applied to those SSCs necessary to prevent criticality events. The highest levels of design, quality assurance, and operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs.

Safety Design Significant SSCs are those needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation. SSCs are also designated as Safety Design Significant if they place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. High levels of design, quality assurance, and operational requirements are applied to Safety Design Significant SSCs.

Additional information on the SSC classification process is provided in ISMP Section 1.3.10, “Classification of Structures, Systems, and Components”.

3.12 Human Factors

In the design of the Project, careful attention is paid at every interface between the operating personnel and the facility to ensure that good human factors and ergonomics practices are followed. This ensures the facility is user-friendly to minimize errors of omission and commission and to ensure the operator is in the best possible position to respond to those situations in which human response is beneficial or required. Attention is given to the placement of instruments and controls in the control room to ensure that clear and unambiguous indications of facility status to the operators. The acceptability of instruments placement is confirmed by constructing a physical or computer mockup of the panels prior to fabrication of the panels. This mockup ensures that compatibility with human psychology and physical characteristics is achieved and enables the required human tasks to be performed reliably and efficiently.

Human factors specialists conduct human factors reviews of training, operator capabilities, work spaces, and the design of the Safety Design Class and Safety Design Significant SSCs and functions that are judged to be critical to facility performance and that have a high potential for human error. These specialists will have many years of experience on a wide variety of nuclear or chemical facilities, including facilities similar to the RPP-WTP. During the early design phase, the specialists identify opportunities for design improvement and provide recommendations to address human factors principles and processes. The specialists conduct interviews with operations personnel from similar facilities to identify lessons-learned relative to human-machine interfaces. In addition, information from incident databases is used to identify where human-machine interfaces are contributing factors in recorded incidents. Human factors specialists are involved in the specification and use of mockups and models of instrument panels and controls rooms. These specialists are also involved in the performance of task analysis that evaluates the functions to be performed by operating and maintenance personnel against the facility design, procedures, and training.

Task analyses are carried out on operations that involve personnel and required to maintain the safety functions of the facility. This includes analyzing the demands on the operating personnel in terms of perception, decision making, and action. The analyses provide an assessment of the feasibility of the proposed tasks and an input to the design of interfaces in accordance with human capabilities. The results of such task analyses also provide the basis for the development of the design, the operating procedures, and personnel training.

Personnel with safety responsibilities are provided with expectations for their safety functions. These expectations include the responsibilities of the operations personnel who monitor and control facility response to faults as well as the responsibilities of those personnel who perform tests, maintenance, or other activities.

The design effort commences with the general layout of the facility and continues through the detailed design stages for each aspect of human involvement during the life of the facility. Adequate instrumentation in the control room and at local control stations is particularly important to allow operators to detect and correct abnormal conditions. Display systems, panel layouts, and workspace access are also important to ensure that routine and special maintenance can be completed safely.

These considerations support the formation of the basis for interactions with other aspects of human factors design, which include training, the preparation of operating instructions, the proposed staffing levels, and the implications for safety management. In this respect, training of operations personnel and other staff is influenced to ensure compatibility with the proposed facility operating regime, and the operating procedures are developed to ensure full compatibility with the design of the tasks and the design of the equipment. Operating instructions are validated for reliable interpretation and implementation by the user. The validation includes the interactions with initiating, sustaining, and terminating cues. The staffing levels are proposed based on the results of the human factors studies to ensure that adequate levels are achieved at all times.

3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI)

To ensure that the facility meets operational requirements, it is necessary to address issues associated with reliability, availability, maintainability, and inspectability.

Reliability is used as a measure of the ability of an item or system to complete a task, and it is normally expressed as a probability of failure. Reliability is designed in through the use of appropriate design techniques and control of the mode of operation and the environment. Design techniques to be used vary because they are dependent on the specific item or system and the task to be performed. Their purpose is to optimize reliability by the following:

1) Use of proven materials and components
2) Design simplicity
3) Testability
4) Control of manufacturing standards
5) Control of operational mode (e.g., prevention of misuse and overloads)
6) Control of environment (e.g., protection against corrosion and vibration).

Consistent with the process for tailoring hazard controls using the potential radiological and chemical consequences of individual events, reliability is assigned to SSCs based upon the importance of the SSC to the prevention or mitigation of accidents. The significance of accident prevention and mitigation is determined by the severity of the accident to workers or the public. To implement this tailoring in a clear, consistent, and defensible manner, an Implementing Standard for Safety Standards and Requirements Identification was developed. This Implementing Standard includes a Severity Level ranking system which provides the hazard assessment and control teams with a defined way to categorize the potential severity of those events that can result in radiological or hazardous exposure to the workers or the public. The Implementing Standard provides the means by which the hazard assessment and control teams establish target reliabilities for SSCs.

Availability is a measure of the degree to which an item or system is in an operable condition. It is expressed quantitatively as the ratio of the mean time between failures to the sum of the mean time between failures and the mean time to repair. System availability is calculated to determine the potential for downtime. In this way, systems are identified that contribute to decreased availability. Required availability is achieved by specifying additional systems or increasing reliability of existing systems.

Maintainability is a measure of the ability to restore a failed item or system to an operable condition in a specified time. Maintainability is designed into the facility and processes through use of appropriate design techniques, (e.g., the use of specially designed, remotely removable, and replaceable pumps and valves in process systems, and the placement of active pumps or valves within shielded accessible areas equipped with appropriate decontamination facilities that allow hands-on maintenance activities) and logistic support (e.g., scheduling and procedures). Benefits of these design techniques are that they simplify maintenance operations in high radiation areas and remove high maintenance equipment from high radiation areas.

Testability of Safety Design Class systems and components is facilitated by such features as redundancy that allow for a system or component to be removed from service for maintenance or testing without loss of safety protection.

Inspectability is the measure of the ease with which items or systems can be inspected for preventative maintenance or assessment of condition. Inspectability is used to monitor facility items in order to maintain their reliability. Inspectability of facility items can be designed in by the use of shielded access areas (as above, to reduce radiation exposure) for active equipment or the provision of monitoring equipment (e.g., material coupons for determining vessel corrosion rates, and in-cell cameras).

During the design phase, the RPP-WTP and processes are evaluated for reliability, availability, maintainability, and inspectability. BNI uses a number of validated modeling techniques (computer codes, mathematical modeling, failure modes, and effects analysis) for determining reliability and availability of the facility and processes. These are used to identify those facility and process areas that are sensitive with respect to influencing overall facility and process performance. Optimum reliability is established by the use of appropriate standards and quality control. The determination of maintenance and inspection needs is based on facility and process reliability requirements. It is a mixture of process optimization, provision of appropriate design features to aid preventative and scheduled maintenance and inspection, and the development of maintenance and inspection programs (administrative and procedural controls) whose objectives among other things, are to facilitate these activities. Reliability targets are assigned to SSCs only when a quantitative value has been credited for the reliability of an SSC in safety analysis.

A hypothetical example of the application of RAMI to the RPP-WTP is the cooling water supply system to the technetium/cesium product storage tank. Cooling water is supplied to the this vessel to keep the contents from boiling thereby preventing the release of radionuclides and steam to the ventilation system. Failure of the cooling water system supply could lead to a hazardous situation or, at the least, operability concerns. The system comprises a closed-cycle primary system supplying chilled water to cooling coils within the vessel. Chilled water is supplied via a secondary chilled water circuit and heat exchanger. It should be noted that physical considerations indicate that the tank contents may reach their boiling temperature, but the predicted time required is on the order of several days. A conservative estimate of the minimum time to boiling assumes there is no heat transfer from the tank (ISAR Section 4.7.2.4, “Technetium/Cesium Product Storage Tank”).

This supply system is analyzed using a commercially available computer program. The system is first broken down into major components (e.g., pumps and valves); for each component reliability data are obtained and an acceptable repair time specified. The computer model calculates total availability of the system throughout the “operating life” of many years. The overall reliability of the system is then determined by application of fault tree analysis. Failure rates for postulated faults are determined and sensitive items of the system with respect to failures are identified.

No maintainability of the in-cell components (primary circuit) is required, as the design takes this into account (e.g., all welded pipework and enhanced testing). Inspection of the primary circuit takes place either indirectly through the use of coupons within the circuit to assess corrosion rates of the pipework and cooling coils or directly through visual (closed circuit television) means.

3.14 Commissioning and Operation

A structured test program ensures that SSCs function correctly against their specific performance requirements, including safety functions. The test program depends on the facility design being systemized, which allows each individual system to be fully tested in isolation before being integrated with the others leading towards full facility operation. Design documentation, such as process and system descriptions, are used as a resource to develop the startup testing program. Full facility operation is dependent on the successful demonstration of the process performed by the facility. Facility operation is not initiated until the systems testing adequately demonstrates their performance objectives in support of the process. Fault detection sooner rather than later is the philosophy to ensure cost-effective design, manufacture, and fabrication, leading to a structured design and testing methodology with the emphasis on systems analysis early in the design process. The RPP-WTP is systemized for design and procurement, allowing the BNI design and testing philosophy to be applied consistently with the Tank Farm facility.

The RPP-WTP includes chemical process and mechanical handling operations, performed by a number of mechanical, electrical, instrument, and control systems contained within a suitable civil structure. Each system is tested to demonstrate performance, as scheduled by a test plan, and is only integrated with other systems when test acceptance criteria have been met.

During testing, diagnostic data are collected, and the initial operating parameters recorded. Operating points are adjusted to conform to the design basis of the system or component. Deficiencies detected in testing are tracked to ensure their resolution.

The method of testing is predetermined to be either analysis, demonstration, or examination, depending on the function performed and the type of SSC. Testing begins at the component level. Only components that have met qualification requirements are integrated into their respective system. Each system is tested, as appropriate, with particular attention given to the system interface(s) with its associated system(s). These interfaces are simulated for the purposes of testing.

Manufactured systems and components are typically tested at their point of fabrication, and held there until proven acceptable for delivery to the construction site. All installed systems are subject to installation and startup tests, to ensure that they perform as they did at their point of manufacture, and that they have not been damaged during transit. These tests include energizing equipment and checking mechanical operation, instrument calibration, electrical cable continuity, and pipe and structural integrity.

A phased testing program is implemented for the RPP-WTP, with the testing schedule established by the availability of systems and their dependence on associated systems. Specific tests are implemented for each system including testing of the supporting or supported systems. Interface testing is of prime importance to the success of testing in this phased manner because the consequences of failure affects the overall schedule. System integration only occurs when each end of an interface has been adequately tested to give confidence that integration will succeed.

When systems have sufficiently demonstrated their ability to function, process operation may begin. A series of system performance demonstrations (SPD) are typically performed to commission new facilities, and the number of SPDs depends on the function of the facility and the materials handled. For the RPP-WTP, the following four levels of SPD are demonstrated:

1) Process systems using water (cold test)
2) Mechanical handling systems (cold test)
3) Facility operation using simulants (cold test)
4) Facility operation using active materials (hot test).

All SPD levels are not applied for all systems and components. For example, the first level would not be applied to the melters or vent systems.

Because the fourth-level SPD is the first time that the facility becomes radioactive, faults identified during previous testing can be corrected without any decontamination costs or radiological hazards. On successful completion of the fourth-level SPD, the facility is ready for normal operations.

The involvement of operations personnel throughout the design process and the involvement of design engineering personnel through the beginning of operations when the facility is turned over to operations are key elements in the design and testing philosophy. The development of facility control system simulators in advance of facility testing also strengthens the ability and confidence in the performance of the facility control systems and operator interfaces.

Such simulators have several purposes: they allow testing of the control systems software offline, without risk to personnel or the facility; they permit proving of the testing, commissioning, and operational procedures and documentation; and they facilitate training of operational and maintenance personnel so they may support testing. Integration of design and operating personnel during testing is important to the successful turnover of the facility for operations because it ensures a relatively smooth transition. These activities ensure that the facility is able to demonstrate operational readiness independently of the testing schedule and in advance of hot testing activities.

3.15 Training and Qualification

Training plays an important role in the safe operation of the RPP-WTP by ensuring that personnel have sufficient knowledge to safely fulfill the roles and responsibilities of their assigned jobs. Operator training for normal operation takes benefit of facility design information, results from the startup test program, operation of similar facilities, and operation of Project demonstration facilities. Training for accident conditions is based, in part, on the safety analyses performed for the RPP-WTP including the hazard analysis and accident consequence analyses.

The training objectives include the following:

1) Improving technical ability (understanding of processes)
2) Enhancing of personal skills (communication, worker-management)
3) Increasing awareness of the workplace and signs of potential hazardous situations

4) Educating personnel in the importance of acting with regard to their own safety and the safety of others
5) Establishing a safety culture that assigns safety responsibility to the individual.

A training plan, described in ISAR Section 3.4, "Training and Qualification", incorporates the above objectives. The plan notes the following requirements that constitute a thorough approach to personnel training and qualification for the RPP-WTP.

1) Recognition of the different types of training that is required. For example achievement of a necessary level of job competence, knowledge of the requirements of applicable laws and regulations pertaining to the handling of radioactive and chemical materials, specialist training for maintenance activities, and detailed knowledge of process operations.
2) Assessment of training needs. Training is most effective when matched to the needs of the individual. This can happen with two-way communication between the training section and the individual. Each person is assessed on training needs, in conjunction with their line management and training personnel. These needs vary from individual to individual and are dependent on job type.
3) Clear definition of responsibility for training. The plan outlines which functional office within the Project is responsible for training and how this responsibility for training was assigned. Personnel are encouraged to take an active interest in their own training and development and are able to discuss with their line management how their needs can best be met.
4) The establishment of learning objectives. These objectives are derived from analyses that describe the desired performance after training.
5) Training requirements evolve as the facility and its safety program evolves. As the facility and process develop from design to testing and operations, and lessons learned from other facilities become available, training information and requirements change. For example, facility operators may need training in a new type of process developed as a result of a facility modification during operations. The training program is flexible to reflect changing requirements. However, training is continuous to reflect these changing requirements and to ensure that job proficiency is maintained; it is not driven solely by changes to administrative or engineered controls.
6) Training evaluation. A feedback process is established to ensure current training needs are being met by assessing the following:
   a) The training being given is appropriate for the task and effective (i.e., individuals learn from the training)
   b) Personnel performance in the job setting
   c) Requirements for new or updated training are being met.
7) Auditability. The training program and individual development are visible. The maintenance of training log books and regular appraisal of an individuals training needs are important in demonstrating that the RPP-WTP personnel are always correctly trained in the current procedures. The training program is evaluated by oral testing, written exams, or assessment of the work product.

Training and qualification credited for public and worker safety are in accordance with the requirements of the QAM. The program for establishing the qualification requirements for RPP-WTP personnel is summarized in ISMP Section 6.1.3, "Personnel Qualification and Resources". Details on the training and qualification programs are described in ISAR Section 3.4, "Training and Qualification".

3.16 Internal Safety Oversight

Internal safety oversight for the Project involves several oversight functions to ensure safety of the public and workers and to preclude environmental degradation. These internal safety oversight functions include corporate safety assessments, management assessments, independent assessments and audits, safety committees, incident investigations, maintenance of the authorization basis, and the USQ process. In ISMP Section 5.4, "Compliance Audits", and Chapter 10.0, "Assessments", other facets of internal safety oversight are covered. Several administrative functions provide information on the adequacy of the oversight functions and also provide information used to define the scope of future internal safety oversight functions. This information includes: performance monitoring; performance indicators; lessons learned and industry experience; and feedback and trending.

The staff possess the unique skills to perform internal safety oversight. Some of the skills applied are as follows:

1) Conducting performance-based assessments that emphasize work activity in progress
2) Reporting deficient conditions to line management
3) Following up on corrective actions to prevent a recurrence of the deficiency
4) Applying performance trending to determine existence of programmatic issues and plan for future oversight areas
5) Understanding the requirements of the Price Anderson Amendments Act and 10 CFR 820, "Procedural Rules for DOE Nuclear Activities"
6) Assisting line management to establish a positive safety culture
7) Incorporating applicable lessons learned from previous RPP-WTP incidents and industry experience at other DOE sites and the commercial power industry to the project oversight program
8) Maintaining a continuing interaction with the RPP-WTP regulator on the status and direction of project oversight activities.

Internal oversight may include participation of staff external to BNI. The external members are selected based on their experience and qualifications to provide different perspectives or expertise in specific functional areas.

3.16.1 Safety Committees

The Project Safety Committee (PSC) structure provides the overview, review, and approval functions for nuclear, radiological, and process safety, occupational safety, and environmental protection matters. The RPP-WTP contractor Executive Committee addresses corporate safety policies and matters as they relate to the Project. The RPP-WTP PSC addresses RPP-WTP-specific safety policies and regulatory requirements. This two-tier structure affords open communications and sharing of relevant information between the corporate staff and the Project.

During the design and construction phase, the Executive Committee and the RPP-WTP PSC focus on nuclear, radiological, and process safety (as related to the development of the facility design and operations) and on worker safety (as related to construction activities). As the construction phase nears completion, the safety committees' focus shifts to commissioning activities and preparations by the various Project organizations to ensure the effectiveness of their nuclear and worker safety programs during operation. During operation, the committees focus on operations, management, performance of personnel, equipment, and systems, and incidence reporting. Near the end of waste processing operations, radiological control and worker safety during deactivation also are addressed.

As part of safety communication throughout the Project, workers will be invited to participate in the safety committee meetings (e.g., during regular updates on worker safety performance, review of proposed corrective actions for incidents involving worker activities). Facility operators also serve as active members on other RPP-WTP safety committees.

3.16.1.1 RPP-WTP Contractor Executive Committee

The RPP-WTP Contractor Executive Committee provides independent oversight and review of Project matters that affect nuclear, radiological, and process safety; occupational safety; and environmental protection. The membership comprises the RPP-WTP Project Manager and senior level management of the RPP-WTP Contractor corporate organization. To accomplish its objective, the Executive Committee periodically reviews areas such as:

1) Safety programs that implement RPP-WTP policy and regulatory requirements applicable to the Project
2) Recommendation of the approval to proceed with hot operations
3) The significance of new regulations applied to Project programs, procedures, and policies
4) Unusual and off-normal incident reports
5) Reports and meeting minutes issued by the PSC
6) The effectiveness of Project safety programs and associated management controls.

The Executive Committee also initiates special independent assessments or audits, as necessary, to obtain additional information concerning the effectiveness of programs or management controls at the Project.

3.16.1.2 Project Safety Committee

The PSC provides advice to the Project Manager on matters related to safety. PSC members are specified from facility management and staff. Specialists in specific fields and external subject matter experts may also be specified, as required. The members are specified from several different organizations and backgrounds to ensure that advice on safety matters is representative of an integrated evaluation of the matters under consideration.

The PSC Chairperson coordinates and facilitates the committee decision making process to achieve consensus on decisions and recommends approval by the Project Manager or designee.

The PSC reviews the management and the performance of the RPP-WTP nuclear, radiological, process, and occupational safety and environmental protection activities, including the following:

1) Results from the Safety Improvement Program
2) Identification, resolution, and implementation of recommendations and corrective actions resulting from nonconforming items or activities, incident investigations, audits and assessments, inspections and reviews, or emergency exercises
3) Unusual and off-normal incident reports, including TSR violations
4) Reports covering such topics as proposed RPP-WTP modifications, emergency exercises, and the implementation of findings from management assessments
5) Performance indicators and trends of the RPP-WTP for worker, public, and environmental safety activities
6) Results of training programs for safety-related activities
7) Operating problems
8) Effectiveness of the safety/engineering interface with respect to the incorporation of safety and environmental requirement in the design.

The PSC is also responsible for reviewing and recommending approval to the Project Manager or his designee, for safety-related documents, such as the following:

1) Proposed changes to the authorization basis
2) Positive USQ determinations prior to submittal to the regulator
3) Procedure development processes and selected facility procedures
4) Proposed Important-to-Safety design changes
5) Responses to Notices of Violations from the regulator
6) Authorization requests and other regulatory submittals
7) State of Washington permits and license applications
8) RPP-WTP pre-operational testing programs including summaries of test procedures and test results

The PSC reviews audit and assessment reports and recommends actions.

The PSC may make use of subcommittees, as appropriate, to provide oversight to specific functional areas or complete specific tasks or evaluations.

3.16.2 Safety Improvement Program

A safety improvement program is developed and implemented by the PSC. The key theme in the safety improvement program is that it is owned by all RPP-WTP personnel with the demonstrable commitment and leadership of senior RPP-WTP management.

The safety improvement program is coordinated, monitored, and implemented by the following:

1) The establishment of the PSC to oversee safety performance
2) The establishment of safety improvement groups to identify and implement improvement initiatives within their work area
3) The senior management support and demonstrated commitment to the PSC by attendance at committee meetings
4) The reviews of safety performance and implementation of safety improvement action plans about four times per year via an appropriately constituted review group established by the PSC. Representatives are selected based on the scope of the review, personnel expertise required for the review, and personnel qualifications.

3.16.3 Incident Investigations

Incident investigations involve the identification, categorization, notification, reporting, and processing of information related to incidents, emergency events, and accidents associated with the RPP-WTP. Incident reports are sent to the DOE Occurrence Reporting and Processing System. Although the incident reporting process is usually initiated with operation of a nuclear facility, the process is developed and implemented for the RPP-WTP construction and testing activities in preparation for operation.

The incident investigation and reporting procedures, and the training to these procedures, ensure that the RPP-WTP regulator, the DOE Program Office, and RPP-WTP management are kept informed on a timely basis, of events and conditions during construction, testing, and operational activities that could adversely affect quality assurance, security, environment, operations, or the health and safety of the public and workers. Incident reports are evaluated for a potential noncompliance to a nuclear safety requirement reportable by the requirements of 10 CFR 820 “Procedural Rules for DOE Nuclear Activities”.

For an incident that indicates a potential inadequacy of previous safety analyses as defined in an approved safety analysis report or that indicates a possible reduction in safety margins as defined in the TSRs, actions are taken to place or maintain the facility in a safe state and a safety evaluation is performed. The completed safety evaluation is submitted to the regulator before removing any operational restrictions initiated in response to the incident.

Additional detail on incident investigations is included in ISMP Section 5.6.7, "Investigation of Incidents" and ISAR Section 3.7, "Incident Investigations".

3.16.4 Unreviewed Safety Questions

1) The probability of occurrence or the radiological or chemical consequences of an accident or malfunction of equipment important to safety, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis, may be increased
2) A possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis, may be created
3) Any margin of safety is reduced.

Proposed temporary or permanent changes to administrative and engineered controls are reviewed by qualified USQ evaluators to determine if they would involve a USQ. An activity will not be undertaken without DOE review and approval if the initiation of the activity would itself involve an unreviewed safety question. If the proposed change does involve a USQ, one of the following three options are pursued.

1) The proposed activity is abandoned.
2) The proposed activity is modified to remove the USQ.
3) The proposed activity is submitted to the regulator for review and approval prior to completion of the activity.

The following organizations have key roles in the RPP-WTP USQ process.

1) The ES&H Organization is responsible for the developing the USQ procedure, developing the training and qualification requirements for USQ evaluators, and maintaining the list of qualified evaluators.
2) The Facility Manager approves the USQ procedure and the training and qualification requirements for USQ evaluators.
3) The Configuration Management Organization is responsible for establishing and implementing the process by which proposed changes, tests, and experiments are reviewed by the USQ process.
4) The PSC approves USQ determinations prior to their submittal to the regulator.

3.16.5 Performance Monitoring

Performance monitoring is used at the RPP-WTP to verify that ES&H and other RPP-WTP programs, plans, and procedures exist; are in place; are adequate; are functioning as designed; and are in compliance with applicable regulatory or permit requirements. Performance monitoring is conducted by a RPP-WTP multidisciplinary team consisting of quality assurance, environmental protection, industrial safety, process safety, health physics, nuclear safety, and regulatory staff. Performance monitoring includes, but is not limited to, reviewing records, plans, and procedures; visually observing operations/activities; and interviewing key personnel. Findings are provided in written reports with recommendations for improvements as applicable. During design and construction, the findings are provided to the Project Manager and during pre-operational testing, operation, and deactivation, the findings are provided to the Facility Manager.

Performance monitoring is conducted to ensure high standards of performance in the following areas:

1) RPP-WTP site monitoring program
2) Health and safety program
3) Personnel training program
4) Employee concerns program
5) Hazardous material inventory and waste tracking systems
6) Facility safety requirements
7) Conduct of operations and maintenance
8) Environmental program
9) Housekeeping
10) Employee compliance to established safety and quality criteria (See ISMP Section 3.4, “Safety/Quality Culture”)
11) Quality Assurance Program.

3.16.6 Performance Indicators

Performance indicators for safety and environmental protection objectives are established for the Project. Performance is monitored on a periodic basis to determine progress of the Project in achieving these indicators. Examples of performance indicators are as follows:

1) A change in the number of lost-time accidents and recordable injuries
2) Radiological exposures of facility personnel
3) Radiation workers exceeding a specified annual exposure level
4) Operation outside the established limits for discharge and disposal of waste
5) Entry into TSR actions statements for reasons other than TSR-required surveillance

6) Violations of TSRs
7) Findings of audits and assessments
8) Unusual incidents
9) Maintenance backlog
10) Effectiveness of the maintenance program (e.g., time to repair, control room annunciators, and equipment out of service)
11) Fire impairments.

3.16.7 Lessons Learned

The lessons-learned program, established and maintained by the ES&H Organization, includes the identification, documentation, validation, and dissemination of lessons-learned information from the Project. An industry experience program that draws on lessons learned, events, deficiencies, and other similar information from other operating sites for the purpose of enhancing the safety of the facility will be established early in Part B.

This information is used in the revision of applicable procedures, development of training curricula, and in the modification of training materials. Personnel potentially affected by lessons-learned material can participate in this training process by providing feedback on information distributed and identifying information for potential inclusion in the process.

3.16.8 Feedback and Trending

As described above, incidents occurring in the RPP-WTP are used as lessons learned to feed relevant information back to appropriate RPP-WTP staff members and the training programs to assist in precluding recurrence. The lessons learned are applied in a broad manner within the RPP-WTP, rather than focused only on the specific administrative or engineered control involved in the incident. Significant lessons learned are provided to the Project Manager during design and construction and to the Facility Manager during operation and deactivation.

Trending within various performance areas, such as operations, training, and maintenance, is used to verify that continuous improvement is being achieved in the Project. In the event that repeat events, findings, or other deficiencies are indicated, follow-up actions are initiated to identify additional corrective actions needed to preclude further recurrence. These additional corrective actions are tracked to completion and their adequacy to correct adverse trends is verified. Adverse trends are also evaluated to determine the existence of a programmatic failure of nuclear safety requirements subject to reporting in accordance with 10 CFR 820, “Procedural Rules for DOE Nuclear Activities”.

4.0 Standards-Based Management

This chapter summarizes the development of the safety management processes and describes how activities and documentation are tailored to the identified hazards and hazardous situations.

4.1 Safety Management Processes

The Project safety management processes are developed through the safety approach as described in Integrated Safety Management Plan (ISMP) Chapter 1.0, "Project Safety Approach", and shown in Figure 1-1.

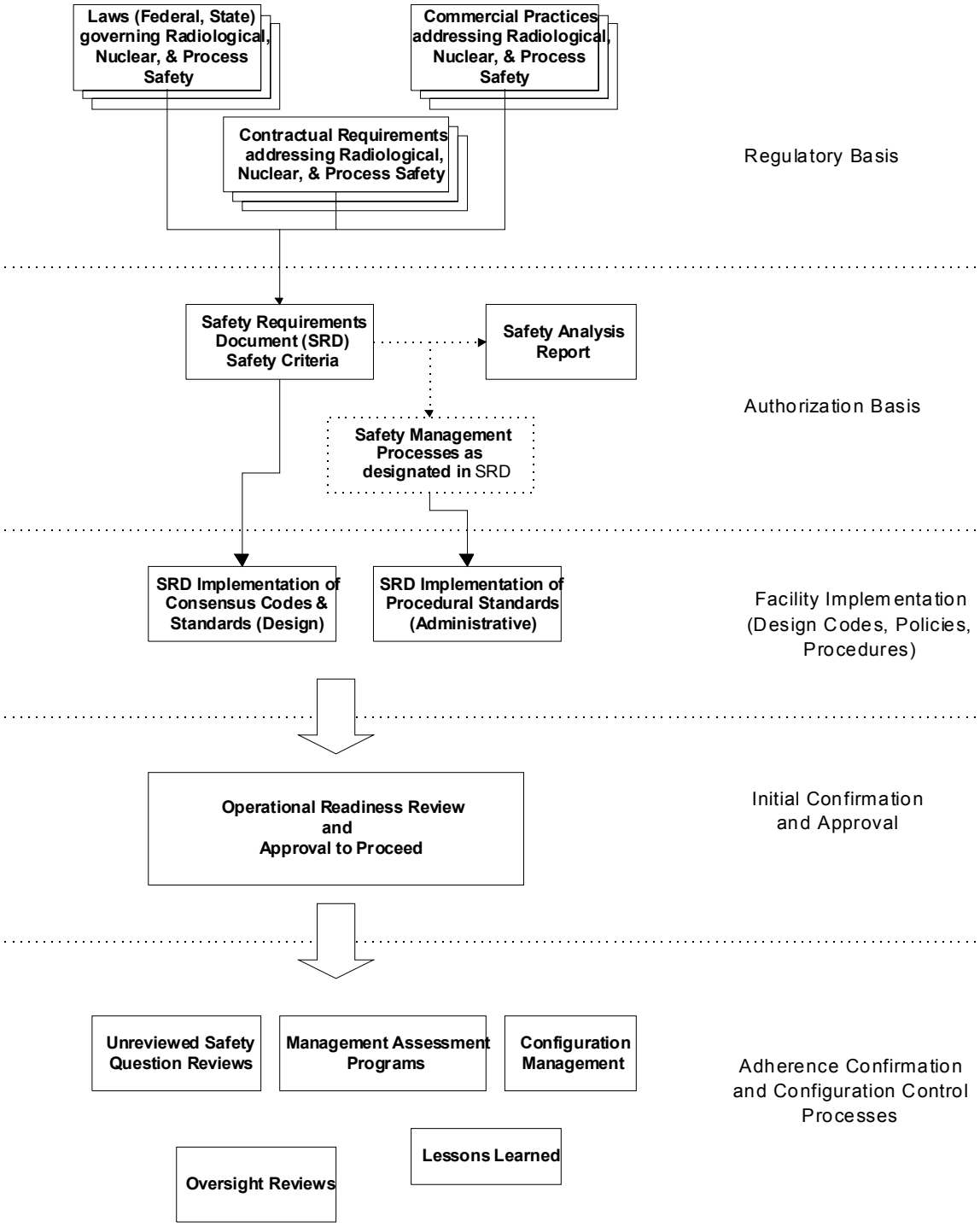
4.1.1 Development of Safety Management Processes

The safety management processes governing radiological, nuclear, and process safety are identified and developed as a part of the Safety Requirements Document (SRD) as shown in Figure 4-1. The SRD development process is discussed in the *Safety Requirements Document* (BNI 2001b).

Development of the Standards-Based Safety Management Programs through the safety approach as part of the SRD development has the following benefits:

1) Continually integrates hazards identification, SRD development, design development, and accident analysis during all phases of the facility life cycle through deactivation
2) Documents the safety management process drivers within the SRD. It also ensures the processes are established in accordance with the applicable regulatory, commercial, and U.S. Department of Energy (DOE) standards and the DOE Top-Level Safety Principles as appropriate to control hazards and hazardous situations associated with the RPP-WTP.
3) Adopts the use of "best industry practices" that include process safety management, a rigorous design process based on a set of credible accidents and a defense-in-depth philosophy, and verification of the level of facility safety through safety analysis and validation of requirements implementation
4) Documents that the facility design meets the required Safety Criteria and documents how and why the engineered and administrative controls credited for public and worker safety were identified. In Part B, when policies and procedures are written to implement the administrative controls, these policies and procedures will be identified in the SRD.

Figure 4-1 Safety Management Processes



4.1.2 Identification of Safety Management Program Drivers

Through the SRD development process, the following safety management programs are identified that:

1) Directly implement regulatory requirements for programs that provide protection of the public and workers from radiological, nuclear, and process hazards (e.g., Risk Management Plan, Radiation Protection Program)
2) Are credited for providing adequate protection to the worker or public (e.g., Emergency Preparedness Program)
3) Place controls on the design, operations, or maintenance of structures, systems, and components (SSC) that are credited for providing adequate protection to the worker or public (e.g., Configuration Management, Conduct of Operations, Quality Assurance, Maintenance).

The following sections outline the programs and identify the SRD sections governing the development of the safety management programs for the RPP-WTP.

4.1.2.1 Nuclear and Process Safety Program

The Nuclear and Process Safety Program addresses the Project integrated approach to nuclear and process safety. It identifies the methodology and Safety Criteria for assessing that the risks posed by the operation of the RPP-WTP are within the overall safety objectives and commitments. The Nuclear and Process Safety Program addresses the following attributes: prevention of accidents, accident and operations risk goals, defense-in-depth, hazards analysis; accident analysis; and criticality. These programs are defined in the SRD Volume II, Chapters 1.0 “Radiological, Nuclear, and Process Safety Objectives”, and 3.0 “Nuclear and Process Safety”.

4.1.2.2 Engineering and Design Programs

The Engineering and Design Program provides the principles governing the design of and identifying design expectations for those SSCs credited for protection of the public and workers. The engineering and design programs include topics such as the configuration management of facility and system design, design practices and procedures for SSCs credited for protection of public and workers, and the facility’s fire protection program. These programs are defined in the SRD Volume II, Chapter 4.0, “Engineering and Design”.

4.1.2.3 Radiation Protection Program

The Radiation Protection Program addresses the protection of the public and workers (when accessing controlled areas) in accordance with 10 CFR 835, *Occupational Radiation Protection*. The Environmental Radiation Protection Program addresses the protection of the public and the environment from normal activities that may release radiological effluents. These programs are defined in the SRD Volume II, Chapter 5.0, “Radiation Protection”.

4.1.2.4 Commissioning Program

The Commissioning Program addresses those requirements applicable to startup of the RPP-WTP and to other operational processes. Commissioning program topics include equipment and system acceptance, pre-operational testing, and validation of operational procedures. This program is defined in the SRD Volume II, Chapter 6.0, "Startup".

4.1.2.5 Management and Operations Program

The safety management programs covered under the umbrella of Management and Operations Programs address programs that establish principles governing the conduct of day-to-day operations which are important in maintaining a safe facility. Included in these programs are the following topics:

1) Management and organization
2) Training, qualification, and procedures
3) Commitment tracking
4) Quality assurance
5) Management assessments
6) Lessons learned
7) Unreviewed safety questions
8) Conduct of operations
9) Conduct of maintenance
10) Employee feedback
11) Incident investigation and reporting
12) Emergency preparedness.

These programs are defined in the SRD Volume II, Chapter 7.0, "Management and Operations".

4.1.2.6 Deactivation and Decommissioning Program

The Deactivation and Decommissioning Program addresses the commitment for deactivation and the design and operational considerations for decommissioning. As the facility approaches deactivation, requirements that provide adequate safety for the activities and inherent hazards of the deactivation process are added to the SRD. This program is defined in the SRD Volume II, Chapter 8.0, "Deactivation and Decommissioning".

4.1.3 Development of Safety Management Programs

The majority of policies, procedures, and instructions fully defining the safety management programs will be developed prior to commissioning of the RPP-WTP. Procedural development will be based on accepted industry practices for ensuring safety through adequate training, conduct of operations, and engineering and design programs. Procedures will be developed internally by the responsible Project organizations.

When developed, these policies, procedures, and instructions (administrative standards) are linked to the driver requirements (Safety Criteria) contained in the SRD. This linking of implementing standards to Safety Criteria ensures that the safety management programs, as defined in the SRD, are fully implemented.

In addition, the consensus codes and standards used in the design of SSCs are linked to SRD Safety Criteria. This link is implemented through Project documents like the Design Input Memorandum. Design guides provide additional detailed project-specific guidance and specifications for topical areas (e.g., radiation protection, human factors, natural phenomena design) and individual systems and areas of the facility (e.g., process ventilation system, melter cell walls, process offgas). All of these links are controlled to ensure that configuration management of the linkage to the SRD is maintained at all times.

Figure 4-2 shows the implementation of the SRD through the design process using these guidance documents.

A key feature of the SRD process is the ability to effect changes to the SRD (when such a change is appropriate). As shown in Figure 4-3, these SRD changes may arise as a result of design evolution or may be identified through the hazard evaluation process. Changes of the first type occur when a proposed design position offers benefits (cost, safety, reliability) but is not fully in compliance with the SRD as written. Changes of the second type may result from newly identified accidents or off normal conditions (indicated by dashed boxes). In either case, all activities are documented, and no change to the SRD is initiated without a formal review for compliance with the standards and requirements on which the SRD is based.

4.1.4 Compliance to and Maintenance of Safety Management Programs

The SRD applies to BNI project contractors.

Compliance to a standard which is included in Volume II of the SRD means that all mandatory statements (shall/will/must) applicable to nuclear, radiological, or process safety are implemented or deviations justified and approved by the DOE. Compliance with non-mandatory statements (should/may) are not required; but are reviewed and considered for each standard on an individual basis. This review is documented. Compliance to statements not applicable to nuclear, radiological, or process safety may in many cases be required to ensure compliance to regulations outside the scope of the DOE review (e.g., environmental protection); however, if no other regulatory entity requires compliance via the standard, compliance is not required to be reviewed on an individual basis.

Safety Management Programs will be scrutinized and revised, as appropriate, as a part of the biannual SRD revision process. This revision process incorporates updated hazards and design information as well as potential new regulatory requirements. This biannual review will ensure that the safety management programs are appropriately tailored to the hazards posed by the facility and comply with laws, regulations, and contractual commitments.

In addition, linking the implementing procedures to the SRD Safety Criteria provide a means of ensuring that revisions to these procedures are reviewed to confirm the safety management programs remain implemented.

Figure 4-2 SRD Link to Design

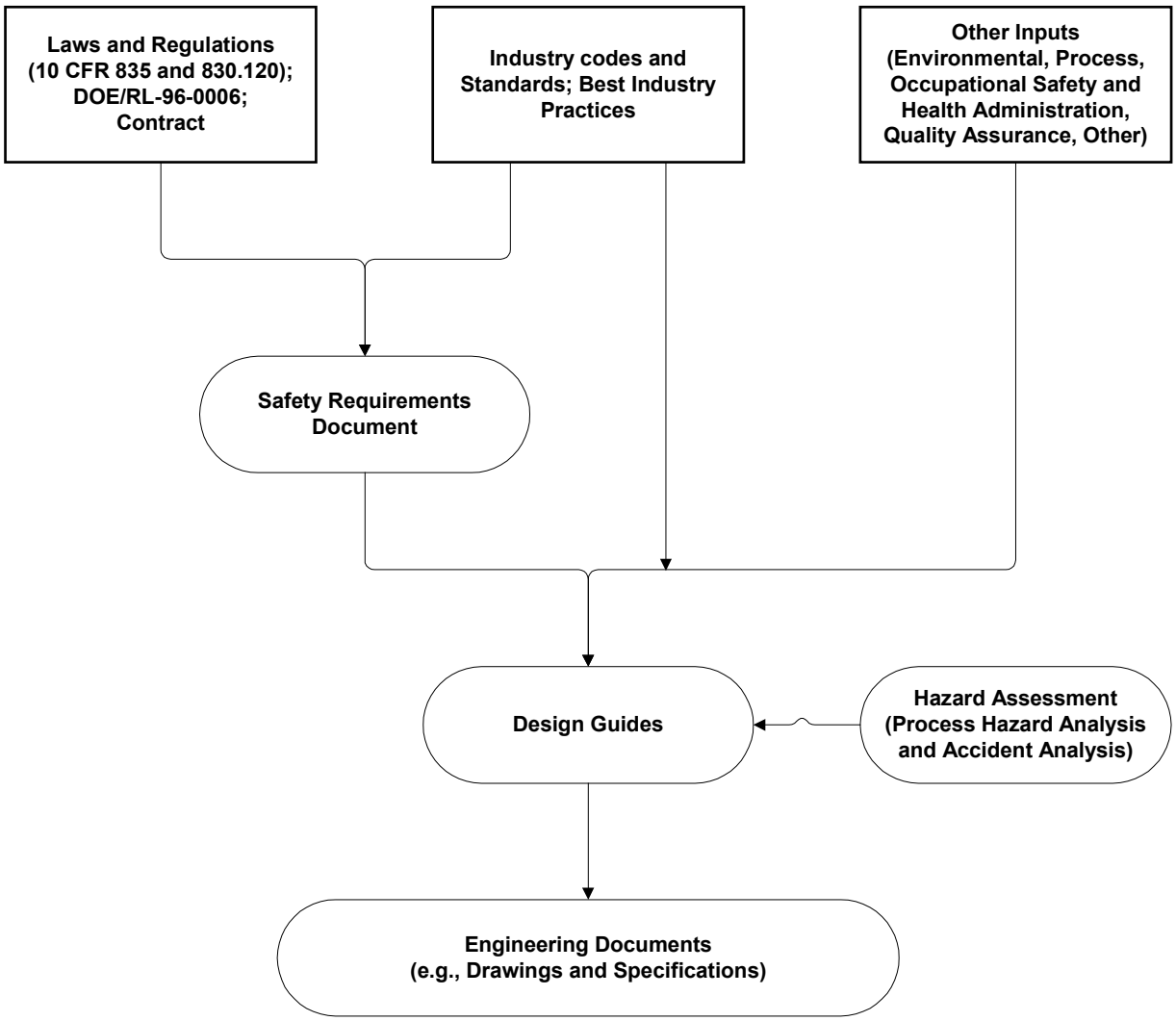
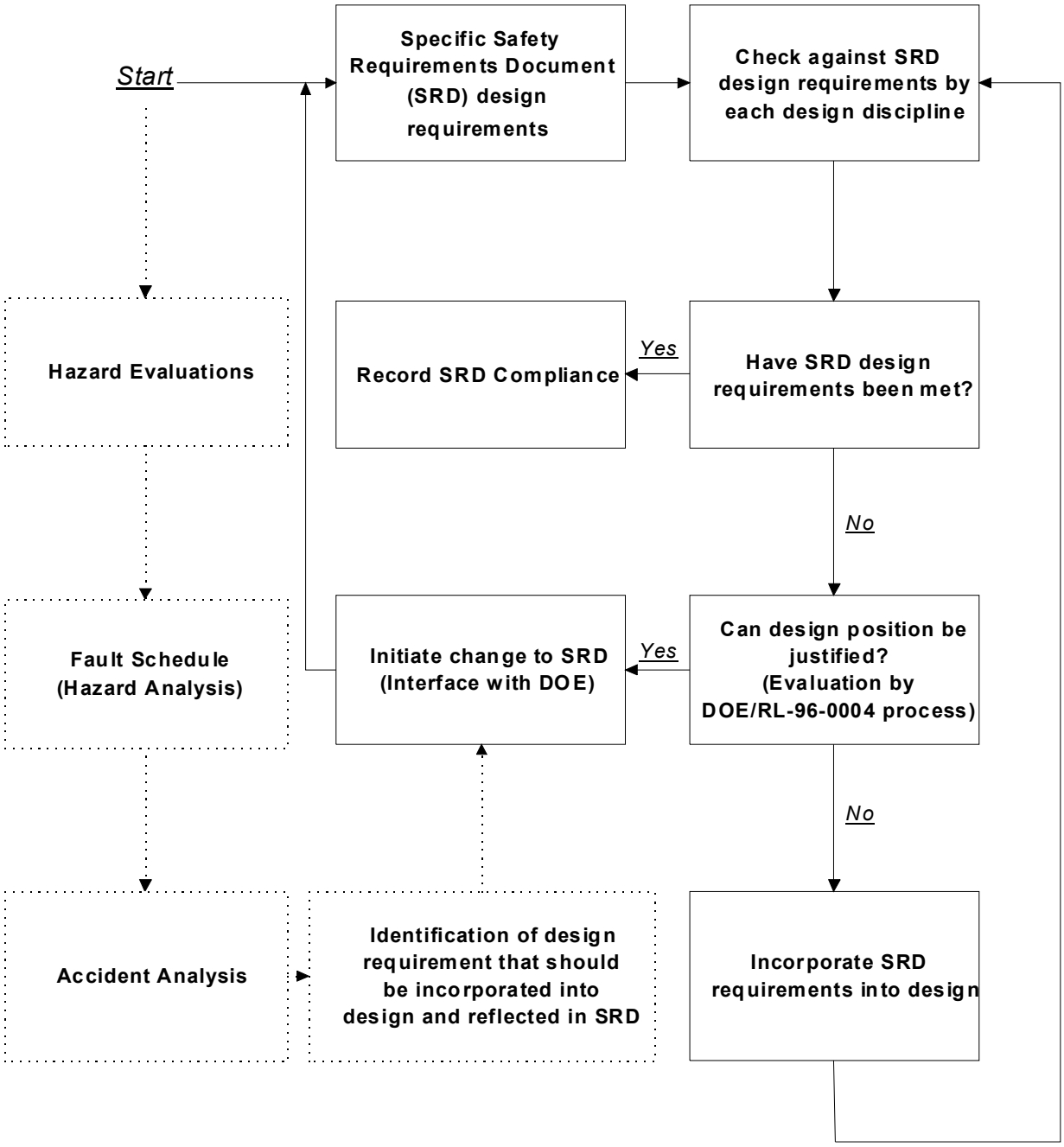


Figure 4-3 SRD Change Process



Proposed changes to the SRD are evaluated for impact on safety compliance with regulations and the authorization basis (including hazard and accident analysis) and then are reviewed and approved commensurate with the process applied to the original configuration, including regulatory approval before implementing changes that could be considered as decreasing the prescribed level of safety. The essential elements of DOE/RL-96-0004 *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, as addressed in the original development of the SRD, are maintained, including the use of subject matter experts and the use of an equivalent level or review and approval of the proposed change. Changes are made by an established configuration management process.

4.2 Tailoring Safety Management Processes

The aspects of the RPP-WTP design that are critical to safety are identified through Process Hazard Analysis (PHA). This process is a systematic team-based review of the facility and process designs that identifies hazards and hazardous situations to a level of detail commensurate with the available design detail. Major hazards and hazardous situations are identified as the level of design detail increases and additional PHAs are performed in Part B. Having generated the list of hazards and hazardous situations, this list is subject to a further systematic team-based review where a binning process takes place.

Hazardous situations are assessed and binned according to a qualitative, and experience, and team-based judgement of frequency and consequence (severity). This binning process receives benefit from the BNI team's experience with safety analysis and operation. Frequency bands are defined and labeled as normal, anticipated, unlikely, and extremely unlikely. Consequences range from negligible through minor to serious and major. The binning process is essentially risk based with categories of hazard defined according to a frequency/consequence matrix. This approach is consistent with the American Institute of Chemical Engineers (AIChE) guidelines on hazard evaluation (AIChE 1992). The binning process assigns hazards as acceptable, acceptable with controls, undesirable, or unacceptable.

In this way, a hierarchy of hazards and hazardous situations is identified. This hierarchy is reviewed and, where possible, the design is modified to eliminate hazards. Where this cannot be done, protection systems are identified that would prevent, protect against, or mitigate the hazardous situation. Protection systems would be a combination of engineered features (e.g., alarms, trips, and interlocks) and administrative controls (i.e., operator actions).

The application of protection systems is tailored to the hazard severity. For example, high-frequency hazards with severe consequences have protection systems involving diverse engineered features and training and procedures requirements as discussed in Section 4.2.2, "Training and Procedures". Less significant hazards would require fewer protection systems that may lean heavily on administrative procedures, the importance of which will have been stressed through adequate worker training. This ensures the appropriate level of safety is provided.

4.2.1 Engineered Features

Engineered features include SSCs that provide for public and worker safety. The design, fabrication, construction, installation, testing, operation, maintenance, and quality assurance requirements for engineered features are tailored by the classification process discussed in ISMP Section 1.3.10, "Classification of Structures, Systems, and Components".

4.2.2 Training and Procedures

Operator training and procedures ensure that the facility is operated safely. The development of the training and procedures during facility design and commissioning takes account of the differing safety requirements. Procedures support the safe operation of the facility in varying ways. A hierarchy of procedures is developed that reflects the level of safety importance. Factors that determine the level of safety importance for training and procedures include support they provide for maintaining compliance to the Technical Safety Requirements (TSR) and maintenance of Safety Design Class and Safety Design Significant SSCs. Those at the highest level are subject to increased rigor with respect to their development and implementation. Increased rigor means independent review and endorsement by suitably qualified and experienced personnel or safety committees. All procedures that have an impact on the safe operation of the facility are developed and implemented with a suitable degree of rigor commensurate with their safety importance.

Operator training and qualification requirements are tailored to operator requirements. Facility area operators are trained and qualified in their specific areas of operation, radiological and chemical hazards, and necessary emergency requirements (facility recovery and facility and site evacuation). Facility supervisors and operators with increased responsibility receive additional training (e.g., in specific operations, resetting of facility items required for safety, and emergency response). Training ensures that operators receive the necessary knowledge and experience to conduct operations with due regard for safety. Training of maintenance and technical personnel is tailored to the involvement of these personnel in the establishment and maintenance of administrative and engineered controls. More in-depth and frequent training is provided for those individuals involved with Safety Design Class and Safety Design Significant engineered features.

4.2.3 Tailoring of Safety-Related Documentation

The following sections describe how the safety analysis reports (SAR), Integrated Safety Management Plan (ISMP), Safety Requirements Document (SRD), TSRs, and emergency plan are tailored to the phases, hazards and hazardous situations of the RPP-WTP.

4.2.3.1 Safety Analysis Reports. The format and content of the Preliminary Safety Analysis Report (PSAR) and Final Safety Analysis Report (FSAR) are in accordance with *Safety Requirements Document Volume II*, section 9.1, "Safety Analysis Reports" and the implementing standards referenced in section 9.1. To facilitate the review of the SARs by the regulator, the SAR content also gives consideration to the review guidance developed by DOE. For the PSAR this guidance is provided in *Review Guidance for the Construction Authorization Request (CAR)* (DOE-RL 2001).

The format and content of the SARs are tailored to the nature of the RPP-WTP relative to the hazards and hazardous situations identified by the PHA.

Table 4-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 (this table has been deleted)

All text on this page has been deleted.

All text on this page has been deleted.

The content of the PSAR and FSAR is tailored to the purpose of these two documents. The PSAR supports the request for the construction authorization by documenting the safety criteria, the principal design and construction requirements, and the initial safety analysis. The FSAR documents application of these criteria to the completed RPP-WTP, documents the final safety analysis, and establishes the facility can be operated safely. The PSAR places greater emphasis on design criteria and construction practices than conduct of operations. The FSAR places emphasis on conduct of operations.

Table 4-2 Planned Differences Between PSAR and FSAR Content (this table has been deleted)

All text on this page has been deleted.

All text on this page has been deleted.

All text on this page has been deleted.

All text on this page has been deleted.

All text on this page has been deleted.

All text on this page has been deleted.

All text on this page has been deleted.

4.2.3.2 Integrated Safety Management Plan

The ISMP is tailored to the various phases of the Project. It is currently focused on design and construction. However, ISMP Sections 1.3.14, "Commissioning" through 1.3.19, "Deactivation" address integrated safety management for the Project throughout the life cycle of the project (i.e., from commissioning through deactivation). In addition, the administrative controls developed for design and construction (such as training and procedures, configuration management, incident investigation, and quality assurance), are applicable to the operations and deactivation phases. As the project nears operation, the ISMP is revised to give greater attention to the conduct of operations, operational assessments, incident reporting, and maintaining the authorization basis for the facility. Near the end of waste-processing operations, the ISMP is revised again to address the hazards associated with deactivation. This ISMP revision also discusses the integration between the various deactivation activities, such as preparation of the deactivation management plan; development of the deactivation baseline, end point criteria, and surveillance and maintenance requirements; updating of the PHA; and proposed revisions to TSRs.

4.2.3.3 Safety Requirements Document

The SRD is tailored to reflect adequate control of hazards and hazardous situations associated with RPP-WTP operation. This tailoring activity includes identifying only those Safety Criteria that are required to accomplish Project activities safely, and then applying the implementing codes and standards to these criteria based on the risks posed by the hazardous situations being controlled. Features controlling hazardous situations with the potential for greater impacts (such as an offsite release affecting the public) have more rigor applied to them than those features controlling hazardous situations with lower impacts.

4.2.3.4 Technical Safety Requirements

The TSRs are based on the FSAR and any facility-specific commitments made. They are tailored to focus on the protection of public and worker health and safety. The TSRs are further tailored based on the following needs:

1) Control process variables, design features, and operating restrictions that are initial conditions (i.e., the assumed facility state) for accident analysis credited for meeting the public and worker radiological or chemical exposure standards
2) Assure that SSCs credited for achieving compliance to public and worker radiological and chemical exposure standards will function when required.

The TSRs are kept current so that they reflect the facility as it exists and as it is analyzed in the FSAR. The RPP-WTP is operated to the approved TSRs.

As the RPP-WTP operation nears the end of waste-processing operations, changes are initiated to the TSRs to control the hazards and hazardous situations associated with deactivation.

4.2.3.5 Emergency Plan

The RPP-WTP emergency management plan documents the provisions for response to operating emergencies. The emergency plan establishes effective and efficient emergency management operations that provide acceptable levels of protection for RPP-WTP workers, Hanford Site employees, and the public. The scope of the RPP-WTP emergency management program, from which the emergency plan is derived, is determined by performing a Hazards Survey and Assessment for the facility.

The Hazards Survey briefly describes the potential impacts of emergency events or conditions and summarizes applicable federal, state, and local planning and preparedness requirements. The Hazards Survey identifies the required scope of the RPP-WTP emergency management program.

If the Hazards Survey identifies hazardous materials at the facility in excess of predetermined thresholds, a facility-specific Hazards Assessment is performed. A Hazards Assessment includes the identification and characterization of hazardous materials specific to the facility, analyses of potential accidents or events, and evaluation of potential consequences. The Hazards Assessment provides the technical basis for the RPP-WTP emergency management program and includes information sufficient to determine the scope and extent of the specific elements that make up the emergency management program. These program elements, along with their bases, are documented in the emergency plan. The extent of planning and preparedness directly corresponds to the type and scope of hazards present and the potential consequences of accidents and events.

5.0 Process Safety Management

The Facility may contain highly hazardous chemicals in amounts that exceed the thresholds listed by the Occupational Safety and Health Administration (OSHA) in 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals" (the Process Safety Management [PSM] Standard). Among these chemicals are, for example, anhydrous ammonia and nitric acid. If threshold quantities of hazardous chemicals were exceeded, it would be necessary to develop a PSM program that complies with OSHA requirements and with similar requirements of the prevention program in the U.S. Environmental Protection Agency (EPA) Risk Management Program, 40 CFR 68, "Chemical Accident Prevention Provisions".

Even though compliance with 29 CFR 1910.119 and 40 CFR 68 does not apply to the RPP-WTP, the Project must comply with the top-level process safety management principles in Section 5.0 of DOE/RL-96-0006, *Top Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b). Because the top-level principles mirror most of the elements of the PSM standard (with the exception of employee involvement and trade secrets), a program that satisfies the OSHA PSM standard also satisfies the top-level principles.

This chapter focuses on the management systems that ensure the RPP-WTP operates safely, from the perspective of applying commercial industry practices and approaches that are compliant with PSM.

5.1 Process Safety Information

A compilation of written process safety information is maintained to enable the RPP-WTP employees involved in operating processes to identify and understand the hazards posed by those processes involving hazardous chemicals. The following information is retained:

1) Toxicity information
2) Permissible exposure standards
3) Physical data
4) Reactivity data
5) Corrosivity data
6) Thermal and chemical stability data
7) An assessment of the effects of inadvertently mixing different materials

Most of this information is available in Material Safety Data Sheets, which are made accessible to all employees. Information on interactions is prepared in the form of an interaction matrix developed for the Process Hazard Analysis (PHA). The interaction matrix for the RPP-WTP is provided in Section 4.2, "Chemical Interactions", of the Hazard Analysis Report (HAR). A list of the process chemicals used in the RPP-WTP and their hazardous characteristics is also provided in the HAR Section 4.1.2, "Process Chemicals".

Information pertaining to the technology of the process is also required. This information includes the following:

1) Block flow diagrams and simplified process flow diagrams
2) The process chemistry
3) The maximum intended inventory
4) Safe upper and lower limits for such variables as temperatures, pressures, flows, and compositions
5) An evaluation of the consequences of deviations, including effects on the health and safety of employees.

Process technology information is developed as the design evolves. Confirmation that the process safety equipment is appropriate for the process operation is established from engineering review of the completed design and the updated hazard and accident analysis. Changes in the technology are reviewed by PHAs and controlled by the configuration management process.

Another group of information is required that pertains to equipment in the process. This information includes the following:

1) Materials of construction
2) Process and instrumentation diagrams
3) Electrical classification
4) Relief system and design basis
5) Ventilation system design
6) The design codes and standards employed
7) Material and energy balances
8) Safety systems (e.g., interlocks and detection or suppression systems).

This information is assembled as the design evolves.

The RPP-WTP configuration management system ensures that Process Safety Information is maintained and kept up to date. Section 1.3.16, "Configuration Management", of the Integrated Safety Management Plan (ISMP) provides a summary of the Facility configuration management program. Additional details on this program are provided in Initial Safety Analysis Report (ISAR) Section 3.1, "Configuration Management".

5.2 Control of Subcontractors

BNI is responsible for ensuring that all subcontractors work as safely as the BNI employees. BNI's responsibilities include the following:

1) Informing the subcontractors of known fire, explosion, or toxic hazards relating to the subcontractor's work and the process
2) Explaining to the subcontractor the applicable provisions of the emergency plan
3) Developing and implementing safe work practices to control the entrance, presence, and exit of subcontractor employees, including their presence in areas of the process covered by the PSM standard
4) Periodically evaluating the performance of subcontractors in fulfilling their obligations as stated
5) Maintaining an illness and injury log relating to the subcontractor work in the process areas

Each subcontractor's responsibilities include the following:

1) Ensuring that subcontractor employees are trained in the work practices necessary to safely perform their assignments
2) Ensuring that subcontractor employees are instructed in the known hazards of the process as related to their job assignments, and in the relevant provisions of the emergency management plan
3) Documenting that each subcontractor employee has received and understood the training required to work safely at the RPP-WTP
4) Ensuring that each subcontractor employee follow the safety rules of the RPP-WTP and the site safe work practices, and advise the contractor of any unique hazards presented or found during the course of the subcontractor's work

Project environment, safety, and health (ES&H) requirements are imposed on subcontractors in contracting documents. This includes commitments included in the SRD and ISMP. Subcontractors are required to appoint an ES&H representative who is the interface with the Project team on all ES&H matters.

Before starting any work, ES&H personnel meet with the subcontractor's workers to apprise them of the job-specific ES&H requirements. In addition, oversight is provided of all subcontractor safety and compliance activities.

The system employed on the Project to track subcontractor work includes procedures with detailed checklists and specific record keeping and reporting requirements. The key elements of this system are subcontractor pre-qualification, worker job-specific training, day-to-day monitoring, and regular reporting to the contractor. These elements are described in the paragraphs that follow.

The QAP requires that subcontractors and suppliers providing services and items Important-to-Safety submit their quality plans to Project QA for review and approval.

The QAM describes how the procurement of items and services is controlled to ensure conformance with specified requirements. Audits of suppliers and subcontractors are described in the QAM.

Controls are established by the Project to ensure that purchased items and services conform to the procurement documents. These controls include provisions for source evaluation and selection, objective evidence of inspection at the subcontractor's source, examination of items or services upon delivery, and assessments. Verifications of subcontractors' and suppliers' activities during fabrication, inspection, testing, and shipment of materials, equipment, and components are planned and performed with the Quality Assurance organization participation to ensure conformance with the purchase order requirements.

Subcontractors and suppliers develop procedures for the disposition of items, materials, and services that do not meet procurement requirements to ensure that incorrect or defective items, materials, and services are not used in the RPP-WTP and that reporting requirements are satisfied. BNI validates that approved suppliers can continue to provide acceptable items and services based on a documented evaluation of their past performance.

Pre-qualification. Subcontracting procedures contain subcontract language to ensure that BNI subcontractors understand their obligation to comply with the Project ES&H programs and procedures and all applicable federal, state, and local requirements. Subcontractors are also required to submit an extensive ES&H history form documenting their capability of meeting these obligations. Subcontractors are also required to submit their safety and health program for Project review. Before work is carried out, subcontractors are required to validate that their workers have current training for the work activities they are to perform. This training must be documented as quality assurance records.

Day-to-day monitoring. The subcontractor's ES&H performance is measured against their contractual obligations and ES&H performance. This oversight is the responsibility of the project team, which includes ES&H professionals familiar with the subcontractor scope and the specific ES&H project requirements. Instructions for compliance oversight are specified in the BNI subcontracting procedures and policies. These procedures also contain guidance to initiate contract termination if a subcontractor is found to be in default of these contract obligations, including failure to respond to ES&H infractions.

Regular reporting. Subcontractors maintain their own records of accidents and illnesses and are responsible for notifying BNI immediately of any lost work day injuries/illnesses, occupational fatalities, OSHA-recordable injuries, hazardous material or radiation exposure, or property damage in excess of $500 occurring in areas under BNI control. Subcontractors are also responsible for environmental compliance as defined by applicable procedures, regulations, and laws. These submittals are reviewed by ES&H professionals to give BNI an early warning of performance degradation and to allow BNI to take effective, preventative action when necessary.

The above approaches are formalized in Project policies, procedures, and instructions. Appropriate training is also provided at all levels including employees, supervisors, and management.

To ensure that BNI subcontractors are performing their work safely, both formal and informal safety reviews and audits are performed. Results of these evaluations are transmitted to both Project management and to the affected subcontractors.

5.3 Configuration Management

The configuration management program ensures that the RPP-WTP establishes and maintains consistency among design requirements, physical configuration, administrative controls, and facility documentation to the technical baseline throughout the operating and deactivation phases. Procedures are developed to manage changes to process chemicals, technology, equipment, and procedures, together with changes to facilities that affect a covered process. The procedures ensure that, prior to a given change, the following considerations are addressed:

1) The need to perform an unreviewed safety question (USQ) evaluation
2) The impact of the proposed change on the authorization basis (i.e., RL/REG-97-13)
3) The technical basis for the proposed change
4) The impact of the change on safety and health
5) Modifications to operating procedures
6) Schedule consideration for completion of the activity
7) The authorization requirements for the proposed change
8) The training of employees who are affected by the change prior to commissioning of the process or the affected part of the process
9) Necessary changes in the process safety information and the authorization basis
10) The potential need for changes to the Technical Safety Requirements
11) Necessary changes to the master equipment list.

In the chemical process industries, the above requirements are addressed by a Management of Change procedure. The Management of Change procedure is considered the central element of PSM and its primary purpose is to ensure that change is managed safely. For the Project, the Management of Change procedure is part of the configuration management system that goes beyond the requirements of 29 CFR 1910.

The ISMP Section 1.3.16, “Configuration Management”, provides a summary of the Facility configuration management program. Additional detail on this program is provided in ISAR Section 3.1, “Configuration Management”.

The configuration management program database includes Safety Design Class and Safety Design Significant SSCs. The database relates design information and requirements to the applicable SSCs and associated documentation. The inter-relational nature is such that proposed or identified changes to any part of the controlled design, configuration, or documentation identifies other affected design, configuration, or documentation entities for which consideration of acceptability of the change must be addressed. Within the database are the performance specifications for Safety Design Class and Safety Design Significant electrical and mechanical equipment. These specifications include the conditions under which the equipment must function during the accident condition (e.g., load, pressure, voltage, temperature, radiation field, and humidity).

A proposed change would be disapproved if:

1) The change was found to compromise safety
2) The change would result in non-compliance with a regulation or law
3) The change would result in non-compliance with the contract.

5.4 Compliance Audits

Compliance audits for the PSM program are conducted by BNI at least once every three years to verify that the procedures, practices, and maintenance activities developed to ensure nuclear and process safety are adequate and being followed. These compliance audits are performed by individuals knowledgeable of the process. The audits are often performed with the aid of a checklist. A report of the audit findings is developed in which corrective actions and their schedule for completion are provided. Additional detail on this program is provided in ISAR Section 3.6, "Audits and Assessments".

5.5 Process Hazards Analysis

The PHA is a key element in achieving and maintaining safety throughout the life of the RPP-WTP. The PHA technique evolves as the design matures. The appropriate technique is chosen by using the methodology recommended by the American Institute of Chemical Engineers (AIChE) in its *Guidelines for Hazards Evaluation Procedures* (AIChE 1992). At the conceptual design stage, a preliminary hazard analysis is used. As the design matures, the chosen technique is the Hazard and Operability (HAZOP) Analysis.

Thus, the PHA technique is tailored to the information available and to the complexity of the RPP-WTP processes. In addition, the chosen techniques are among those in the list of acceptable techniques promulgated by OSHA in 29 CFR 1910.119 (e) (2). A discussion of the hazards analysis techniques selected for the Facility is discussed in HAR Section 3.2, "Selection of a Hazard Evaluation Methodology". Application of the selected techniques is discussed in HAR Section 3.3, "Hazard Evaluation Methodology".

The chosen PHA techniques address the hazards of the process by systematically evaluating potential deviations from design intent caused by the failure of engineered or administrative controls, including appropriate detection methodologies that provide early warning of release. Human factors are addressed by identifying those causes of deviations from design intent that are caused by human error. Further detail on human factors is given in ISMP Section 3.12, "Human Factors".

OSHA also requires that the PHA consider how accidents in the process can affect other areas, such as the control room, office buildings, or other nearby structures and processes. Also, the PHA team considers how external events might affect the process. This is accomplished by considering these siting issues in the context of the causes and consequences of the deviations from design basis. The discussion of causes and consequences includes a review of previous incidents at the site and at similar facilities. For the Facility, considerations for siting are addressed in HAR Section 2.1, "Site Description", and the comparison the results of the PHA to those of other facilities is provided in HAR Section 4.4, "Comparison to Similar Facilities". The consideration of consequences also includes a qualitative evaluation of the possible effects on the health and safety of facility workers.

A written plan will be developed in Part B for participation of employees and their representatives in the conduct of the PHA and other elements of the Project PSM program.

The documentation of the PHA is consistent with the examples of documentation given in the AIChE's *Guidelines for Hazards Evaluation Procedures* (AIChE 1992). The results of the PHA for the Facility are included in HAR Section 6.0, "Hazards Analysis Results Summary".

The results of the PHA are submitted to the regulator for review to support the construction authorization package, operating authorization package, and deactivation request as discussed in ISMP Section 9.2, "Scheduling of Events for Regulatory Submittals". The schedule for these submittals of the PHA is shown in ISMP Figure 9-1. The PHA, including revisions, is maintained by the document control process discussed in Chapter 8.0, "Document Control and Maintenance". Access to the PHA and other PSM information is made available to employees.

The PHA is performed in accordance with the requirements of the Project QAP. This includes establishment of personnel training and qualification requirements, confirming that personnel meet these requirements, application of management reviews, and documentation of results.

5.6 Conformance to Other Top-Level Safety Standards and Principles

This section addresses the attributes of a PSM program dealing with procedures and training, maintenance of the HAR, hot work operations, mechanical integrity, commissioning review, incident investigations, and emergency actions.

5.6.1 Procedure Development

Operating procedures provide clear instructions for safely operating the RPP-WTP during commissioning, normal operations, temporary operations, emergency shutdown, emergency operations, normal shutdown, and process startup following a turnaround or emergency shutdown. The procedures cover conditions under which emergency shutdown is required and assignment of shutdown responsibility to qualified operators, thus ensuring that emergency shutdown is executed in a safe and timely manner.

The procedures consider the consequences of deviations from outside normal operating limits and the steps required to correct those deviations. They contain safety and health considerations, such as the properties of, and hazards presented by, the chemicals used in the process. The procedures also contain the precautions necessary to prevent exposure, including engineered features, administrative controls and personal protective equipment, and control measures to be taken if physical contact or airborne exposure occurs. The procedures also address safety systems and their operation, and control of hazardous chemical inventory levels.

The operating procedures are periodically reviewed for human factors considerations and to ensure that they reflect current operating practice. The operating procedures are readily accessible to employees who work in or maintain a process. Safety Criteria 7.2-6, 7.2-7, and 7.2-8 of Volume II of the Safety Requirements Document (SRD) provide criteria for procedures required to implement PSM.

All operations that may affect safety are carried out in accordance with approved procedures that clearly delineate responsibility. Procedures provide step-by-step instructions on how to operate the facility or equipment routinely and safely. Some procedures are developed prior to the commissioning phase and serve to discipline the testing design intent to confirm facility operation to the design. During this phase, procedures are tested to demonstrate that they provide adequate direction for safe performance of facility operations.

There is a defined hierarchy of operating procedures, the position within which depends the safety significance of the operation to which the procedure refers. For example, procedures supporting the implementation of Technical Safety Requirements (TSR) or credited as defense-in-depth features for accident prevention and mitigation have a greater safety significance than those supporting operations with a lower impact on safety. Operator training emphasizes the importance of this hierarchy as well as the need to follow all procedures to carry out facility operations safely and efficiently.

The term "operating procedures" covers the entire range of procedures important for safe and efficient facility operations, in addition to those that detail routine facility operations. Procedures are provided for maintenance and emergency situations as well as day-to-day operations.

5.6.2 Updating of the Hazard Analysis Report

At least annually after the receipt of hazardous material at the RPP-WTP, the PHA and HAR are updated by a qualified team. This is to assure that the process hazard analysis is consistent with the current process. The PHA and HAR are also updated as required by the configuration management program.

Additional control of the HAR is provided by SRD Safety Criterion 3.1-7 which requires that changes in the processes or assumptions be accurately reflected in the hazards analysis. Changes to process or assumptions occurring between periodic updates of the hazards analysis are governed by the USQ process (described in ISMP Section 3.16.4, "Unreviewed Safety Questions", and described in ISAR Section 3.1, "Configuration Management") and by control of the authorization basis as described in ISMP Section 3.3.2, "Control of the Authorization Basis". The periodic reviews and updates of the hazards analysis are performed in accordance with the Safety Criteria of SRD Volume II, Section 3.1, "Hazards Analysis", governing the conduct of the hazards analyses, as implemented and described in ISAR Section 4.9, "Administrative Control of the Integrated Safety Assessment".

5.6.3 Development of the Operator Training Program

The operator training program is developed and implemented in accordance with SRD Volume II, Section 7.2, "Training and Procedures". Details on the Project training and qualification programs are provided in ISMP Section 3.4, "Safety/Quality Culture", and Section 3.15, "Training and Qualification". ISAR Section 3.4, "Training and Qualification", further addresses the training policy and describes the level of training required to receive to efficiently and safely perform their intended duties.

The BNI program implements the above-referenced SRD criteria which contain a requirement to develop an operator training program that includes an overview of the facility processes and operating procedures, the specific safety and health hazards, operating limits, emergency operations, safe work practices, and refresher training.

Each employee involved in operating a process is trained in an overview of the process and in the operating procedures and instructions. The training includes emphasis on the specific safety and health hazards, operating limits, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.

Refresher training is provided at least every 3 years for PSM activities, and more often if necessary, to each employee involved in operating a process to ensure that the employee understands and adheres to the current operating procedures and instructions of the process and is proficient in the procedures to follow if conditions exceed the design basis of the facility.

5.6.4 Commissioning Review

Prior to operation of the RPP-WTP with radioactive materials and chemicals considered to pose a hazard, commissioning tests of the facility systems and personnel are performed in accordance with the Safety Criteria of SRD Volume II, Section 6.0, "Commissioning". This testing confirms that Safety Design Class and Safety Design Significant structures, systems, and components (SSC) are capable of performing their specified safety functions and personnel are knowledgeable and proficient in the performance of procedures. A review is also performed to ensure that the necessary safety, operating, maintenance, and emergency preparedness procedures are in place and adequate prior to operation of the facility. The content of the commissioning plan is provided in ISAR Section 3.10, "Testing Program and Preoperational Safety Review".

5.6.5 Mechanical Integrity

Procedures are established to maintain the integrity of process equipment, including pressure vessels and storage tanks, piping systems and pipe-mounted components, relief and vent systems and devices, emergency shutdown systems, controls (including monitoring devices and sensors, alarms and interlocks), and pumps. Inspections and tests that follow generally accepted good engineering practices are performed on process equipment. The frequency of inspections and tests is determined by manufacturer's recommendations, good engineering practices, and the vulnerability of components to the effects of aging, modified as necessary by operating experience. Inspection and test results are documented. Equipment deficiencies identified by the inspections or tests are corrected in a safe and timely manner.

The Project training program includes the training of each employee involved in maintaining the integrity of process equipment.

The Project QAP includes requirements for procedures to ensure that equipment, as fabricated, is suitable for the process application for which it will be used. Checks and inspections are performed to ensure that equipment is installed properly, and is consistent with design specifications and the manufacturer's instructions. A spare parts management system ensures that maintenance materials, spare parts, and equipment are suitable for the process application for which they are used.

Central to maintaining chemical and radiological exposures at a minimum is the requirement to maintain the mechanical integrity of SSCs. Maintenance activities related to this requirement are categorized as follows:

1) Routine
2) Planned replacement
3) Preventative
4) On demand (i.e., in response to failures).

The requirement for mechanical integrity is dependent on the duty of the equipment and its accessibility for routine inspection and maintenance. Therefore, in-cell equipment (which resides in a high radiation area) requires a higher level of reliable mechanical integrity than readily accessible out-cell equipment. The other important factor that influences the required degree of integrity is the role of the SSC in accident prevention or mitigation. Appropriate mechanical integrity of facility equipment is ensured using the following methods:

1) Early identification of safety significance and maintenance requirements (e.g., degree of accessibility and reliability)
2) Application of the appropriate manufacturing standards and quality assurance
3) Facility (equipment) acceptance testing
4) Inspection and monitoring requirements (preventative maintenance)
5) Training and maintenance instruction requirements.

5.6.6 Hot Work Operations

Hot work operations are reviewed and conducted in accordance with SRD Safety Criterion 4.5-19 which governs administrative controls to minimize fire hazards. These controls include those governing the use of ignition sources, reviewing proposed work activities for fire protection impacts, and the establishment of compensatory controls for activities that may impair fire prevention or mitigation features. The fire protection program is described in detail in ISAR Section 8.0, “Fire Safety”.

Implementation of other safety work practices, such as system and equipment tagout, use of scaffolding, and confined space entry, are also developed. They are addressed in detail in ISAR Section 3.11, “Operational Practices”.

5.6.7 Investigations of Incidents

For incidents that have the potential to result in a major accident or a release of hazardous or radioactive material from the controlled area of the RPP-WTP, an investigation is conducted in accordance with the Safety Criteria of SRD Volume II, Section 7.7, "Reporting and Incident Investigation". Incidents are categorized as soon as possible and, in all cases, within 2 hours as Emergency, Unusual, and Off-Normal occurrences. When the categorization is not clear, the occurrence is conservatively categorized at the higher level. Investigation of the incident is initiated as promptly as possible, but not later than 48 hours following the incident. The focus of the RPP-WTP incident investigation program is the identification of the events and near misses, determination of root causes, identification of corrective actions, dissemination of information to the lessons learned program, reporting of incidents, and the monitoring of the effectiveness of corrective actions. Additional information on incident investigation is provided in ISMP Section 3.16.3, "Incident Investigations". The incident reporting procedure and additional detail on the incident investigation program is contained in ISAR Section 3.7, "Incident Investigations".

An incident investigation team is established for incidents that have the potential to result in a major accident or a release of hazardous or radioactive material from the controlled area. The team consist of at least one person knowledgeable in the process involved, including a subcontract employee if the incident involved work of the subcontractor, and other persons with appropriate knowledge and experience to thoroughly investigate and analyze the incident. A report is prepared at the conclusion of the investigation. The report is reviewed with all affected personnel whose job tasks are relevant to the incident findings. The incident report includes as a minimum:

1) Date of incident
2) Date investigation began
3) A description of the incident
4) Results of the root cause analysis
5) The factors that contributed to the incident
6) Any recommendations resulting from the investigation.

A system is established to promptly address, resolve, and document the incident report findings and recommendations.

The incident categorization is one factor used in determine the extent of the incident investigation in terms of the size of the investigation team, its independence, and the depth of the root cause analysis. By this process, the extent of the incident investigation is tailored to the consequences of the event or the potential consequences of a "near miss". For example, by tying the incident investigation to the event categorization, an increasing level of investigation is applied to the following events: 1) a hazardous substance release that exceeds 50% of a CERCLA reportable quantity; 2) a chemical release that violates environmental requirements in state or federal permits; and 3) a chemical release that had reported effects on collocated workers.

The categorization process is not the only factor that determines the extent of the incident investigation. For example, incidents that are repeat occurrences will receive more in-depth investigation, in part, to determine the reason for ineffectiveness of the corrective actions. Where repeat incidents or recurring causes are indicated, prompt follow-up action is initiated to identify additional corrective actions needed to preclude recurrence. These additional corrective actions are tracked to completion and their adequacy verified to ensure correction of the problem. An evaluation also is conducted for repeat occurrences to determine if the trend represents a programmatic failure reportable under 10 CFR 820.

The investigative process is used to gain an understanding of the incident, its causes, and corrective actions necessary to prevent recurrence. The process is summarized below.

1) The scope and depth of analysis of a particular incident is tailored to the significance of the incident. The tailoring of the analysis (i.e., incident investigation) is in part dependent on the categorization of the incident, if the incident is a repeat occurrence, and if the incident is considered a significant condition adverse to quality.
2) If the investigative process warrants a team investigation as determined from the evaluation above, at least one member of the investigative team is assigned from the organization most closely involved with the activities that were ongoing at the time of the event or incident. This member provides detailed first-hand knowledge of the performance of the activities. Other members are independent, and all members are knowledgeable of facility design and operations or are experts in safety (industrial or process).
3) At least one member is formally trained in at least one of the various industry-accepted methods of incident investigation and cause determination.
4) The team investigates the event, identifies underlying causes, formulates corrective action recommendations, and documents the results of the investigation.
5) The incident investigation process, its implementation, and its effectiveness are reviewed periodically by the Project Safety Committee or by audits or assessments.

5.6.8 Emergency Action Plan

For accidents that result in the need to take additional actions to protect the public and workers, and the environment from accidental releases of hazardous or radiological material, an emergency response program is provided in accordance with the Safety Criteria of SRD Volume II, Section 7.8, “Emergency Preparedness”. Emergency preparedness is addressed in ISMP Section 3.10, “Emergency Preparedness”. The Emergency Response Plan is outlined in ISAR Section 9.0, “Emergency Management”. This ISAR section describes how the plan complies with the requirements of 29 CFR 1910.38, “Employee Emergency Plans and Fire Protection”, 40 CFR 355, “Emergency Planning and Notification”, DOE/RL-94-02, *Hanford Emergency Response Plan*, (DOE-RL 1994) and DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b).

6.0 Integrated Safety Management

This chapter describes how safety management is integrated into work planning and performance. Lines of responsibility and authority for environment, safety, and health (ES&H) issues are described. Personnel qualification, resource allocation, and hazard assessments, controls, and operating conditions are discussed.

6.1 Integration Into Work Planning and Performance

The Project safety management process protects the public, workers, and the environment through implementing work practices that never compromise safety for the sake of production or expediency. This is achieved by BNI by way of the following:

1) Conduct activities in an atmosphere of trust and confidence based on open, honest, and responsible communication
2) Encourage employee feedback
3) Use proven and effective approaches to risk identification and control
4) Conduct business with integrity and mutual respect for employees and interfacing organizations
5) Apply a systematic approach to all activities that affect ES&H
6) Establish clear ownership and accountability
7) Define and reach agreement with the employees on the work to be accomplished by the facility operation and the expectation to accomplish the work in a safe manner
8) Promote teamwork through involvement of knowledgeable parties
9) Empower employees to effectively protect themselves, the public, and the environment
10) Allocate appropriate resources to support ES&H activities
11) Support continuous improvement of ES&H performance
12) Manage and conduct a consistent and project-wide integrated approach to ES&H for all activities
13) Encourage and promote sharing ES&H information and resources
14) Assignment of a qualified person for overall responsibility for the development, implementation, and integration of the safety management process.

Application of the above work practices allows the BNI team to effectively implement BNI guiding principles for integrating safety management into work planning and performance efforts. These guiding principles include establishing line management responsibility for ES&H, establishing and making clear lines of authority, ensuring that personnel have the necessary qualifications to perform the work, providing effective allocation of resources, performing pre-work hazard assessments, establishing appropriate controls for hazards and hazardous situations, and establishing operational requirements.

These work practices and principles are an integral part of the BNI team safety culture. They are formalized in Project policies, procedures, and instructions and are incorporated into all activities described in the following sections. The flowdown of these work practices and principles to subcontractors is discussed in Section 5.2, "Control of Subcontractors".

6.1.1 Line Management Responsibility for ES&H

Line management responsibility and accountability for ES&H is one of the key principles of the BNI approach to ES&H integration. To ensure maximum effectiveness in ES&H performance, employees are informed of their responsibility and accountability for creating and maintaining a safe and healthy workplace and protecting the environment.

In addition, ES&H individuals do not assume roles that reside with the line organization. This creates an environment where accountability is clearly focused and ES&H priorities are never sacrificed to another line mission or objective.

6.1.2 Lines of Authority and Responsibility

Clear and unambiguous lines of authority and responsibility are established throughout the Project through its design, construction, operation, and deactivation phases. The flowdown of ES&H responsibility and accountability starts with the Project Manager during construction and the Facility Manager during operation (which includes deactivation) and extends through the management and supervisory chain to each worker, irrespective of the type of work being performed. This flowdown is captured in policies and procedures, communicated to the workforce through orientation and training, reinforced by group and individual performance evaluations, and monitored and assessed by independent oversight provided by ES&H professionals.

Stop-work authority also flows down from senior management to individual workers who are explicitly empowered to halt any activity in which they are engaged that is unsafe or potentially harmful to the environment.

6.1.3 Personnel Qualification and Resources

The Project training provides personnel with the knowledge, skills, and direction necessary to perform their duties in a safe and environmentally sound manner. Training is performed using a tailored approach, commensurate with the level of risk and individual responsibility.

The Project training addresses relevant ES&H requirements and is provided at all levels of the organization as follows.

1) Employees are trained to ensure they recognize, understand, and anticipate the hazards and the environmental requirements associated with performing their work.
2) Supervisors are trained to ensure they understand their responsibilities for assisting employees in analyzing the work for safety hazards and environmental compliance requirements; to assist employees in maintaining physical protection at work sites; and to enforce (and reinforce) performance standards, protective measures, and environmental practices.

3) Managers are trained to understand their responsibilities for providing necessary ES&H support and direction to supervisors, employees, and subcontractors and for demonstrating ES&H leadership through their actions and communications.

Resources are assigned to ensure that protection is provided for the public, workers, and the environment. The risk assessment process, discussed in Section 6.1.4, "Hazard Assessments, Controls, and Operating Conditions", provides the key input to the resource allocation process by identifying the significant risks associated with RPP-WTP work activities.

6.1.4 Hazard Assessments, Controls, and Operating Conditions

The performance of hazard assessments, the specification of appropriate controls, and the establishment of safe operating conditions are all achieved through the use of a risk assessment system that ensures that all significant risks are identified. The RPP-WTP risk assessment system evaluates tasks and the work environment to anticipate, recognize, evaluate, and control situations, conflicts, and stressful situations, and other conditions that may significantly affect the health, safety, or efficiency of the Project employees. Each of the following basic components of the systems is performed with a degree of rigor based on the scope of the work effort and commensurate with the potential hazardous situation it presents as follows.

1) Pre-job planning encompasses the task description, expected hazards and hazardous situations, protection methods, anticipated exposure levels, waste generation, and emergency response.
2) Baseline evaluations determine the status of a facility area or system.
3) Integrated hazard analyses detail the evaluations of the potential hazards and the controls needed to protect the public, personnel, and the environment.
4) Radiological work planning outlines routine and special radiological controls, precautions, surveillances, and instructions to personnel, as well as prerequisite conditions (e.g., tagouts and system isolations).
5) Assessments and surveillances including formal and informal appraisals, monitoring, and oversight activities to verify that specific elements of the policies, programs, plans, and procedures are being effectively implemented; that work is being performed safely; and appropriate compliance and commitment tasks are being performed.
6) Investigations of work-related injuries or illnesses, near misses, motor vehicle accidents, property damage, environmental spills and releases, fires, and explosions through accident and incident response to identify the root cause and contributing causes of the event and the corrective actions necessary to prevent recurrence.

The above safety management processes provide a coherent, integrated, and formalized methodology to ensure that the risks associated with potential health, safety, and environmental hazards and hazardous situations are identified and properly addressed, and that the RPP-WTP can be operated safely and in compliance with environmental regulations.

7.0 Regulatory Interfaces

This chapter describes the BNI interface with regulatory agencies regarding environmental protection, occupational health and safety, and safeguards and security. Section 7.4 "Resolution of Conflicting Requirements and Standards" covers the resolution process when standards and requirements conflict.

7.1 Environmental Protection Interface

The U.S. Department of Energy (DOE) and the State of Washington have analyzed the environmental impacts from treatment of tank waste by vitrification in the Tank Waste Remediation System (TWRS) Environmental Impact Statement (EIS). This EIS satisfied both the requirements of the *National Environmental Policy Act* and the *State Environmental Policy Act*. In addition, the Record of Decision (62 FR 8693) for the TWRS-EIS selected the phased implementation option that called for the deployment of two Phase I facilities to treat the tank waste.

To support the Record of Decision resulting from the TWRS-EIS, the BNFL team prepared an environmental report (ER) in accordance with the requirements of 10 CFR 1021.216, "Procurement, Financial Assistance, and Joint Ventures". The environmental report updates the information provided by the DOE and the Washington State Department of Ecology (Ecology) in the EIS.

The Environmental Protection Agency (EPA) has provided Ecology and the Washington Department of Health (DOH) the authority to permit air emissions including those from the Facility. Ecology is responsible for regulating criteria pollutants and toxic air pollutants (WAC 173-460 and 173-400). The DOH regulates radioactive emissions.

Ecology regulates the RPP-WTP with respect to the *Resource Conservation and Recovery Act of 1976* (RCRA). The regulations for the management of dangerous waste are found in WAC 173-303. A contract Part A deliverable is a Draft Dangerous Waste Permit Application for review by the DOE. Many meetings with Ecology to date have focused on the Draft Dangerous Waste Permit Application to obtain early benefit of input from Ecology.

The WTP project team identified all of its environmental permits and monitoring in an Environmental Plan. In addition to the air permits and the Dangerous Waste Permit Application, the plan identified activities to be performed by the team during Part B to protect the environment.

To support early development of the Environmental Plan, the BNFL team prepared a Permitting Plan in conjunction with the DOE, Ecology, and the DOH. This plan provided the tentative dates for major permitting activities for the RPP-WTP. In addition, the Permitting Plan documented all of the permitting interfaces with other DOE waste treatment, storage, and disposal facilities, and provides public involvement opportunities. The Permitting Plan was approved and signed by representation of DOE, Ecology, DOH, and the WTP contractor.

BNI participates in information exchanges with the environmental agencies through routine Permitting Task meetings and workshops. Ecology and the DOH are regular participants in these meetings along with DOE. BNI maintains communication with the regulatory agencies through these meetings, occasional technical meetings on specific topics, and by numerous discussions either in person or by telephone to exchange additional information.

7.2 Occupational Health and Safety Interface

BNI complies with all applicable federal, state, and local safety and health regulations to ensure occupational health and safety for RPP-WTP workers. The project occupational safety and health program is regulated by the US Department of Energy (DOE).

The DOE has drafted a memorandum of understanding with the OSHA for the DOE to provide onsite observation of OSHA compliance similar to that conducted by the U.S. Nuclear Regulatory Commission (NRC) at nuclear reactors. BNI responds to observations provided by the DOE to both the OSHA and the DOE. In addition, any responses to OSHA inquires are sent to both entities.

BNI ensures non-radiological safety and health (i.e., occupational health and safety) compliance with applicable regulations by the design, testing, and maintenance of structures, systems, and components and through administrative controls to address health and safety hazards. The identification and mitigation of occupational health and safety hazards occurs through application of the RPP-WTP Project non-radiological worker health and safety program and, for hazardous materials above threshold quantities, compliance with the Process Safety Management (PSM) regulation found in 29 CFR 1910.119, as discussed in ISMP Section 5.1, “Process Safety Information”. Identification of hazards includes the use of Material Safety Data Sheets and other methods as specified in 29 CFR 1910.1200, “Hazard communication”. The Project maintains records of compliance activities as part of the protocols found in ISMP Chapter 8.0, “Document Control and Maintenance”, to support non-radiological safety and health inspections.

7.3 Safeguards and Security Interface

The preliminary assessment of the composition of candidate radioactive waste feeds indicated the quantities and types of special nuclear materials (SNM) to be handled at the RPP-WTP should be classified as Attractiveness Level E and Nuclear Material Safeguards Category IV. These are the lowest classification levels. Safeguards and security requirements for SNM appropriate for the RPP-WTP will be developed with DOE. These considerations will be consistent with the economic and strategic value of the materials present at the facility. Any conflicts that arise between considerations for safeguards and security and radiological, nuclear, and process safety will be resolved by discussions among BNI and the DOE.

7.4 Resolution of Conflicting Requirements and Standards

Conflicting standards and requirements can arise internal to the radiological, nuclear, and process safety regime and external to this regime. The Project safety management process addresses both types of conflicts as described below.

Internal Conflicts

Internal conflicts are identified as a direct consequence of the Project approach to design. The ISMP Section 4.1.3, "Development of Safety Management Programs", describes how the Safety Requirements Document (SRD) is linked to the design process to ensure that standards are properly implemented. Because all standards and requirements information flows down into lower level design guides (see Figure 4-2), internal conflicts are recognized. At this point, the process established to maintain the SRD is used to resolve the conflict. The process for maintaining the SRD is described in SRD Volume I, Section 3.6, "Maintenance of the SRD".

External Conflicts

To ensure that current regulatory requirements and regulatory changes are promptly and accurately identified, BNI team members maintain access to multiple regulatory resources, as discussed in Section 2.1.

When the potential applicability of an existing, new, or revised regulatory requirement is identified, any conflicts are resolved. The impact on project cost and schedule, along with the feasibility of implementing the requirement, are included in the evaluation.

Routine meetings with the regulator offer a forum for identification and discussion of external conflict issues. Letters between the regulating agencies and the BNI team provide formal documentation of issue resolutions.

In the cases where safety and environmental regulations conflict, absent the granting of an exemption from the regulation, the more stringent regulation is followed.

The nature of taking responsibility for operation of the double-shell tank AP-106 requires the resolution of a number of interface concerns. From an early stage, interface meetings were held among the WTP Project contractor, the DOE, and the Project Hanford Management Contractor (PHMC) to identify and resolve these concerns. Interface responsibilities are agreed on and recorded in interface control documentation. Adding concerns to this documentation and accepting their resolution requires approval of all parties involved with the interface issue.

8.0 Document Control and Maintenance

The Quality Assurance Manual (QAM) requirements for the Project records management system is provided in Section 5, "Instructions, Procedures, and Drawings", Section 6, "Document Control", and Section 17, "QA Records" of the QAM (BNI 2001).

Documents are prepared, reviewed, approved, issued, and revised to prescribe processes, specify requirements, and establish design. Safety documents developed as a part of the safety management process controlled by the QAP include but are not limited to those identified in Table 8-1. The column "Records" lists the documents that address the items in the "Subject" column.

Table 8-1 Safety Management Records (Sheet 1)

Subject	Records
Authorization basis	• Integrated Safety Management Plan • Safety Requirements Document • Radiation Exposure Standard for Workers Under Accident Conditions • Preliminary Safety Analysis Report • Final Safety Analysis Report • Technical Safety Requirements • Quality Assurance Plan and Implementation Plan • Radiation Protection Program • Emergency Plan • Safety Evaluation Reports • Written communication with the regulator • Safety analyses
Design	• Master equipment list • Software verification and validation • Equipment and system testing requirements • Equipment qualification requirements • Facility and equipment description and drawings • Design control procedures • Design Criteria and bases for Safety Design Class and Safety Design Significant structures, systems, and components (SSC) • Records of facility changes (configuration management) and associated integrated safety analyses • Specifications for Safety Design Class and Safety Design Significant SSCs • ALARA documents
Construction	• Records of site characterization measurements and data • Construction procedures • Inspection and test records • Construction material certifications • Calibration and test records • Nonconforming condition reports and closure records • Procurement specifications • Craft qualification records

Table 8-1 Safety Management Records (Sheet 2)

Subject	Records
Management Organization and Administration	• Administrative procedures with safety implications • Performance Plans • Employee concerns program, discipline, and employee action records (for protected activities) • Evidence of deliberate misconduct • Organization charts, position statements, training, and qualification records • Safety and health compliance records, medical records, and personnel exposure records. • Safety statistics and trends • Incident reports • Technical and experience qualifications (design, construction, and operation)
Operations	• Commissioning test results • Operating logs • Maintenance records • Calibration and testing data • Material balance, inventory, transfer, and disposal records • Material storage records • Facility operating procedures • Change control records for Safety Design Class and Safety Design Significant procedures • Operator aids (e.g., charts and drawings used to assist operator in performing job) • Training records • Special test records • Corrective action determination and close-out reports • Unreviewed safety question screening and evaluation reports • Records pertaining to disposal of radioactive and mixed wastes
Integrated Safety Analysis	• Integrated Safety Analyses and supporting data, analyses, calculations, and documents • Change control records for Safety Design Class and Safety Design Significant changes to facility • List of Safety Design Class and Safety Design Significant SSCs • Methods for setting acceptable safety limits and controls (including nuclear criticality safety) • Fire hazard analysis • Initial Safety Analysis Report • Hazard Analysis Report
Radiological Safety	• Radiation protection (and contamination control) records • Radiation Work Permits • Radiation protection training records • Records pertaining to radiological process incidents, unusual incidents, and accidents • Individual monitoring (10 CFR 835.702) • Monitoring and workplace (10 CFR 835.703) • Administrative (10 CFR 835.704) • ALARA records • Dosimetry records • Release of property and equipment • Exposures exceeding applicable limits • Records pertaining to sealed sources, accountability, and control • Receipt and transportation or radioactive materials

Table 8-1 Safety Management Records (Sheet 3)

Subject	Records
Nuclear Criticality Safety	• Nuclear criticality control procedures and statistics* • Records pertaining to nuclear criticality incidents, unusual incidents, and accidents* • Records pertaining to nuclear safety analyses (* criticality analysis may show these records to be unnecessary)
Chemical Safety	• Chemical process safety procedures • Records pertaining to chemical process inspections, audits, investigations, and assessments • Chemical process safety reports and analyses • Chemical process safety training
Fire Safety	• Hot-work permits and fire-watch records • Records pertaining to inspection, maintenance, and testing of fire protection equipment • Records pertaining to fire protection training • Pre-fire emergency plans
Emergency Management	• Review of emergency plan from outside emergency response organizations and supporting entities • Memoranda of understanding with outside emergency response organizations • Records pertaining to the training of personnel involved in emergency preparedness functions • Emergency drill and exercise records • Records pertaining to inspection and maintenance of emergency response equipment and supplies
Environmental Protection	• Environmental release and monitoring records • Environmental Report • Environmental Permits (e.g., air, water, and waste)
Occupational Safety and Health	• Material Safety Data Sheets • Training records of staff and contract employees • Inspection and testing reports • Equipment deficiency reports and resolution
Deactivation and Decommissioning	• Deactivation records • Incident reports to support decommissioning (e.g., radiological and chemical spills)
Quality Assurance	• Training and qualification/certification records • Audit and assessment procedures and reports • Surveillance reports • Nondestructive testing procedures, calibration data, and test results • Calibration results • Nonconforming condition reports and closure documentation • Defective and counterfeit items • Procurement documentation • Supplier assessments and vendor inspections • Project review of vendor drawings • Certified vendor information

9.0 Scheduling of Safety-Related Activities

This chapter provides the sequence of events for safety-related activities and deliverables for the design, fabrication and construction, commissioning, operation, and deactivation phases of the Project. The safety-related activities to be conducted during these phases are also presented.

9.1 Scheduling Safety-Related Activities

Figure 9-1 shows the sequence of events and interdependencies between the safety-related Part B activities. A schedule addressing Figures 2, 5, 6, and 7 of DOE/RL-96-0003, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, (DOE-RL 1996a) was provided in BNFL Inc. letter of November 4, 1998 (reference 000500).

Tables 9-1 through 9-5 describe key safety-related activities and show the assignment of these activities to functional areas.

9.2 Scheduling of Events for Regulatory Submittals

This section addresses the scheduling of regulatory submittals required by DOE/RL-96-0003, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors* (DOE-RL 1996a) and the Safety Requirements Document (BNFL 1997d). Figure 9-1 provides the sequence of events for the following deliverables to DOE.

1) The construction authorization package, which will include the Preliminary Safety Analysis Report (PSAR). The PSAR will address Items 1-5, 7-15, 18, and 20 of DOE/RL-96-0003, Section 4.3.2, "Contractor Input", (DOE-RL 1996a). The remaining items will be provided separately from the PSAR.
2) The operating authorization package, which will include the Final Safety Analysis Report (FSAR). The FSAR will address Items 1-5, 7-9, 12, 15, 17, 18, 20, 21, and 23 of DOE/RL-96-0003, Section 4.4.2, "Contractor Input", (DOE-RL 1996a). The remaining items will be provided separately from the FSAR.
3) The submittal of the deactivation authorization request. This will include revision to the Integrated Safety Management Plan (ISMP) to provide additional detail on deactivation activities.

The self-assessment documents identified in Item 4 of DOE/RL-96-0003, Section 4.5.2, "Contractor Input" are provided to the DOE within 90 days of the completion of the assessment.

Revisions to the Quality Assurance Program will be submitted to the DOE with the standards approval package for construction, operation, and deactivation which is submitted fourteen weeks prior to the scheduled authorization request submittal.

Figure 9-1 Sequence of Safety Related Activities (Sheet 1 of 3)

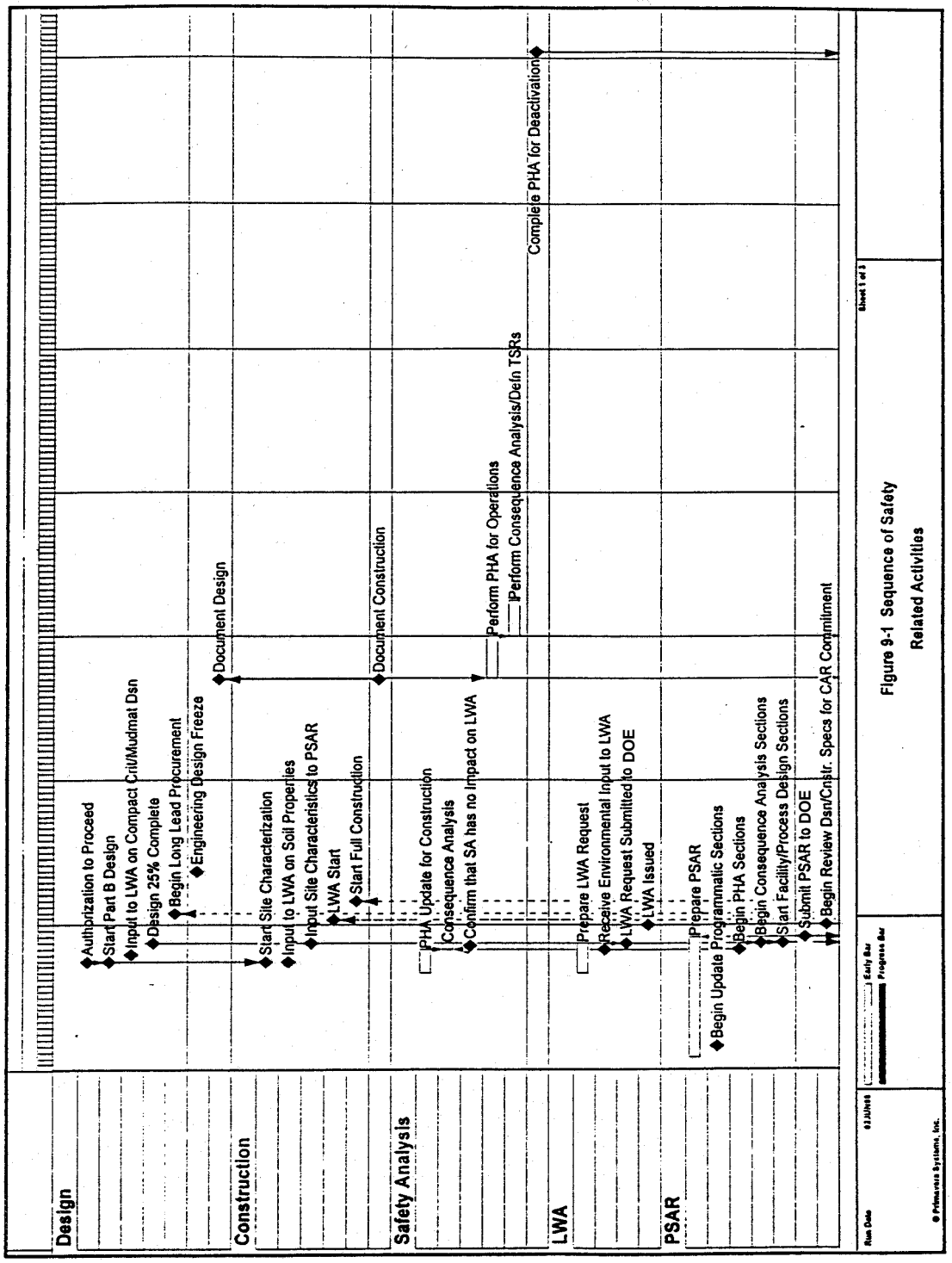


Figure 9-1 Sequence of Safety Related Activities (Sheet 2 of 3)

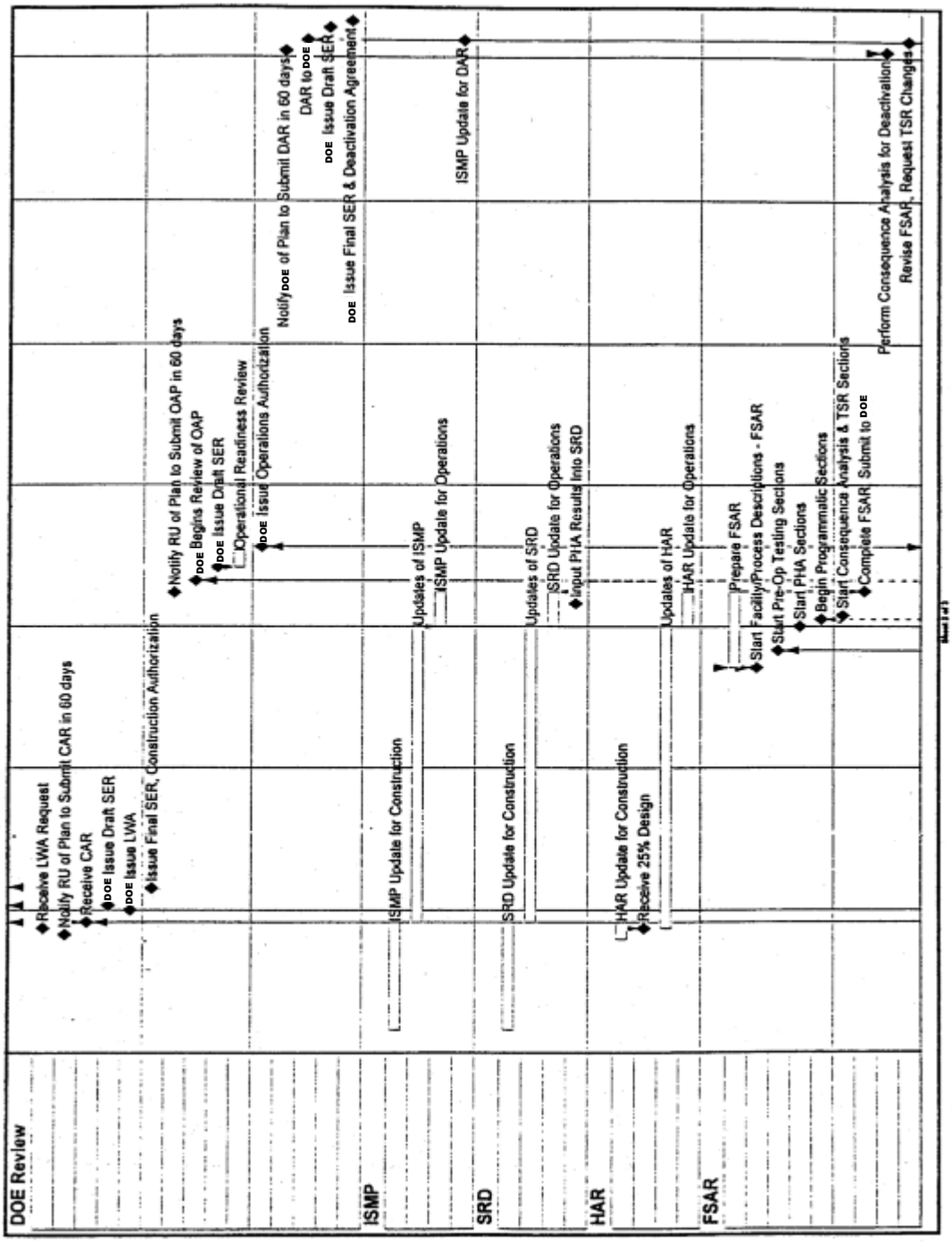


Figure 9-1 Sequence of Safety Related Activities (Sheet 3 of 3)

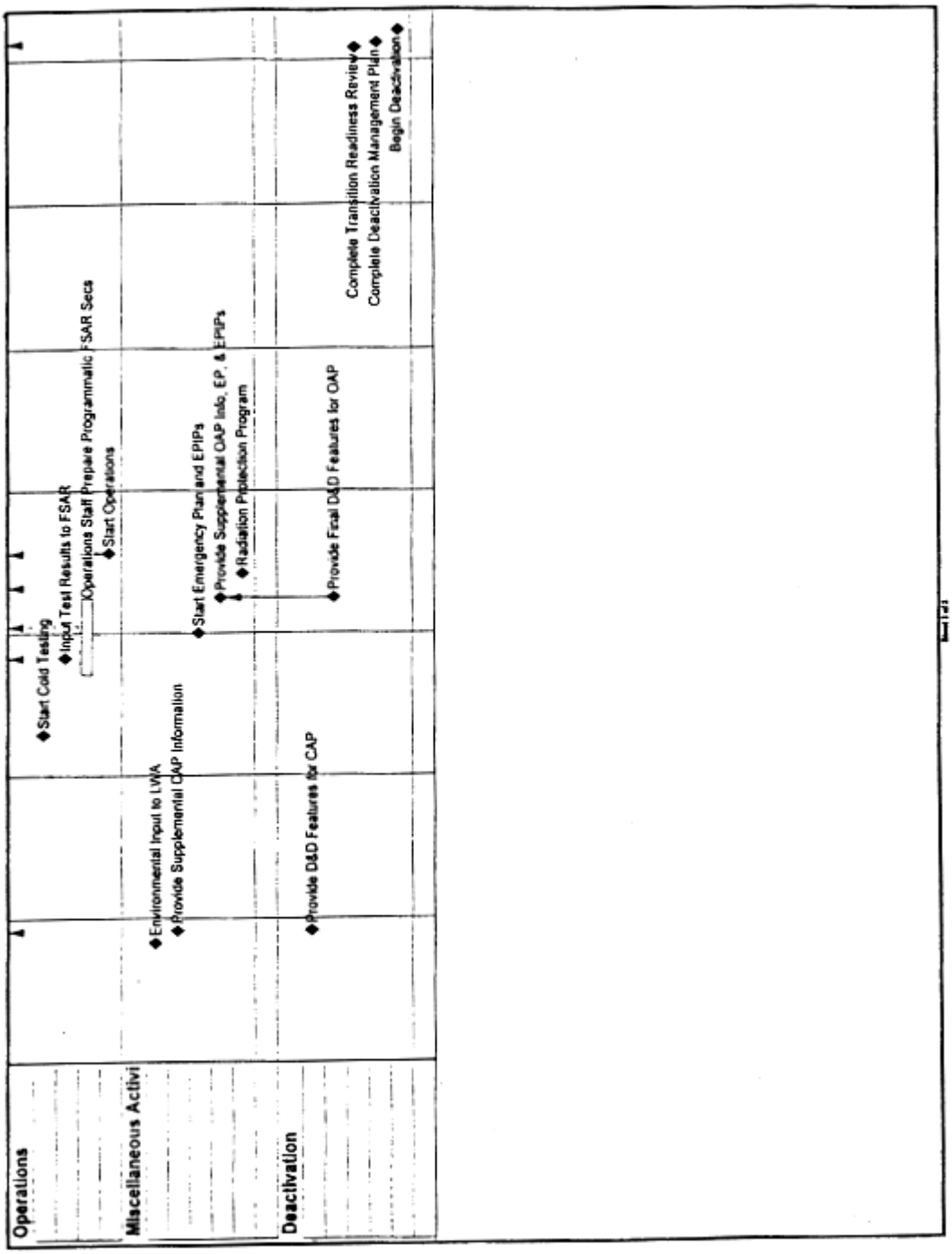


Table 9-1 Key Safety-Related Activities – Design Phase (Sheet 1)

Safety-Related Activities	Functional Area
Planning:	
• Define safety policy and objectives	• Project Management
• Define critical safety interfaces for the various phases of the project	• Project Management
• Implement safety policy and objectives	• Line Managers, all functional areas
• Assign roles for safety-related activities	• Project Management
• Develop procedures to implement safety objectives and organizational plans	• Environment, Safety, and Health
• Develop plans and procedures to address internal safety and oversight functions	• Environment, Safety, and Health
• Develop plans and procedures to address quality assurance and quality control functions	• Quality Assurance
• Develop plans and procedures for identification and resolution of employee concerns	• Human Resources
• Develop performance measures	• Project Management
• Develop employee feedback program	• Project Management
• Develop configuration management program	• Configuration Management
• Develop and implement a regulatory commitment tracking system	• Environment, Safety, and Health
Analysis / Regulatory:	
• Update Process Hazards Analysis (PHA)	• Environment, Safety, and Health
• Update Hazard Analysis Report	• Environment, Safety, and Health
• Identify requirements of the facility design for environmental regulatory compliance	• Environmental Protection
• Identify requirements of the facility design for Occupational, Safety, and Health (OSHA) Administration compliance	• Environment, Safety, and Health
• Prepare applications for state and federal environmental permits	• Environmental Protection
• Update Standards Requirements Document	• Environment, Safety, and Health
• Update Integrated Safety Management Plan	• Environment, Safety, and Health
• Prepare limited work authorization request	• Environment, Safety, and Health
• Prepare Preliminary Safety Analysis Report	• Environment, Safety, and Health

Table 9-1 Key Safety-Related Activities – Design Phase (Sheet 2)

Safety-Related Activities	Functional Area
Design Functions:	
• Develop the quality assurance program plan for the design phase	• Quality Assurance
• Develop facility design that will achieve the defined work activity and satisfy commitments of the construction authorization package	• Engineering
• Incorporate into the design measures that minimize the hazards associated with processing and storing radioactive liquid and solid waste, and fissionable materials	• Engineering
• Incorporate into the design measures to facilitate performance of Technical Safety Requirement surveillances	• Engineering
• Incorporate design features to ensure personnel exposure is as low as reasonably achievable	• Engineering
• Identify design requirements for security	• Environment, Safety, and Health
• Incorporate design requirements for security	• Engineering
• Implement consideration for deactivation and decommissioning into the facility design	• Engineering
• Verify and validate design products against safety requirements	• Engineering
• Implement configuration management control program	• Configuration Management
• Define acceptance criteria for the construction testing program	• Engineering
• Perform systematic design reviews to determine readiness to authorize construction of Safety Design Class and Safety Design Significant systems, structures, and components	• Engineering

Table 9-2 Key Safety-Related Activities – Fabrication and Construction Phase

Safety-Related Activities	Functional Area
Construction:	
• Implement quality assurance program plan for the construction phase	• Quality Assurance
• Incorporate regulatory and quality commitments into procurement, fabrication, inspection, and testing	• Engineering
• Incorporate regulatory requirements and quality commitments into facility construction, procurement, fabrication, inspection, and testing specification, training, and procedures	• Engineering and Construction Management
• Implement procedures and training to enhance construction safety	• Engineering
• Develop a program to ensure that the designer's configuration management program is implemented and that as-built information critical to safety is supplied to the facility operator	• Configuration Management
• Develop procedures for hazardous material handling, packaging, labeling, and shipping practices	• Construction Management
Inspection and Testing:	
• Conduct audits and inspections that verify compliance to requirements by the construction contractor, subcontractors, and Safety Design Class and Safety Design Significant suppliers of systems, structures, and components	• Quality Assurance
• Implement construction testing program to verify that SSCs meet acceptance testing requirements	• Construction Management
• Perform a systematic review(s) to determine readiness to authorize facility turnover in preparation for commissioning testing	• Environment, Safety, and Health

Table 9-3 Key Safety-Related Activities – Commissioning Phase

Safety-Related Activities	Functional Area
Planning:	
• Develop objective and scope for startup testing (scope to include initial and boundary conditions and simulated single failures, as appropriate)	• Technical Support
• Identify the role of design and accident analyses organizations in the identification of the tests to be performed and acceptance of the test results	• Technical Support
• Develop testing program that emphasizes testing with non-radioactive streams	• Operations
• Identify tests to be performed and their acceptance criteria	• Technical Support
• Develop the quality assurance program plan for an operating facility	• Quality Assurance
• Develop operating staff training program	• Operations
• Conduct staff training	• Operations
• Develop program for procedure preparation, review, validation, approval, change, deviation, and internal control	• Operations
• Define the maintenance program that includes preventive, predictive, and corrective maintenance practices and incorporates vendor-recommended maintenance activities	• Technical Support
• Develop operating procedures	• Operations
• Develop administrative procedures	• Operations
• Develop maintenance procedures	• Maintenance
• Develop procedures for hazardous material handling, packaging, labeling, and shipping practices	• Technical Support
• Prepare Final Safety Analysis Report	• Environment, Safety, and Health
• Implement a process safety management program	• Environment, Safety, and Health
Startup Testing:	
• Write test procedures	• Technical Support
• Develop processes for evaluating and resolving unreviewed safety questions and for requesting discretionary enforcement relief from Technical Safety Requirements	• Environment, Safety, and Health
• Perform testing and document results to acceptance criteria	• Operations
• Collect safety component and process baseline data for future performance monitoring and maintenance planning	• Configuration Management

Table 9-4 Key Safety-Related Activities – Operations Phase

Safety-Related Activities	Functional Area
Planning Prior to Facility Operations:	
• Develop Technical Safety Requirement (TSR) surveillance testing and evaluation program	• Environment, Safety, and Health
• Provide independent internal oversight review to ensure facility operation within the authorization basis	• Environment, Safety, and Health
• Develop the radiation protection program	• Radiation Protection
• Develop emergency response procedures	• Operations
Facility Operation:	
• Implement the operational phase quality assurance program	• Quality Assurance
• Implement the emergency preparedness plan including conduct of emergency exercises	• Operations
• Implement the radiological protection program	• Radiation Protection
• Implement a monitoring, evaluation, and reporting program in compliance with the operating authorization	• Environment, Safety, and Health
• Implement the operational phase program for internal safety and oversight functions	• Environment, Safety, and Health
• Implement performance measures and feedback systems	• Facility Management
• Implement a management assessment function	• Facility Management
• Implement a maintenance program	• Maintenance
• Perform testing and monitoring required by the TSRs	• Maintenance
• Operate facility to achieve defined work activity and within the operating authorization and authorization basis	• Facility Manager
• Perform incident investigations including reporting, root cause analyses, identification of corrective actions, and tracking of effectiveness of corrective actions and apply lessons learned from relevant facilities	• Environment, Safety, and Health
• Maintain an operating history to facilitate deactivation of the facility	• Configuration Management

Table 9-5 Key Safety-Related Activities – Deactivation Phase

Safety-Related Activities	Functional Area
Planning:	
• Define deactivation interfaces for surveillance, maintenance, and deactivation	• Technical Support
• Develop the surveillance and maintenance criteria and end point criteria	• Technical Support
• Assign roles and responsibilities for safety-related activities for deactivation	• Facility Manager
• Identify deactivation measures that minimize hazards associated with treating and storing radioactive, liquid, and solid waste, and fissionable materials	• Technical Support
• Prepare deactivation management plan	• Technical Support
• Modify plans and procedures addressing internal safety and oversight functions for deactivation phase	• Environment, Safety, and Health
• Modify plans and procedures addressing quality assurance and quality control functions for the deactivation process	• Quality Assurance
• Develop deactivation performance measures	• Facility Manager/Technical Support
• Develop/modify operating and maintenance instructions for post-deactivation operational equipment	• Maintenance
• Develop design modifications to facilitate deactivation	• Technical Support
Analysis / Regulatory:	
• Perform a job hazard analysis and update the Hazard Analysis Report	• Environment, Safety, and Health
• Identify critical aspects of facility deactivation that would effect environmental regulatory compliance	• Environmental Protection
• Prepare applications for changes to state and federal environmental permits	• Environmental Protection
• Prepare a deactivation Safety Analysis Report and modify facility authorization basis	• Environment, Safety, and Health
Deactivation:	
• Initiate the quality assurance program plan for the deactivation phase of the facility	• Quality Assurance
• Implement facility modifications to facilitate performance of Technical Safety Requirement surveillances	• Technical Support
• Initiate deactivation	• Operations
• Monitor deactivation activities to ensure personnel exposure meets as low as reasonably achievable objectives	• Radiation Protection
• Verify and validate the deactivation process against safety requirements	• Environment, Safety, and Health
• Confirm the facility has achieved a passive state that meets the end point criteria	• Environment, Safety, and Health

During operation of the RPP-WTP, reports will be submitted to DOE that report the following:

1) The quantity of each principal radionuclide in excess of background released to the unrestricted area in liquid and gaseous effluents
2) The calculated annual dose to the maximally exposed members of the public
3) The calculated collective dose to members of the public.

In addition, the PHA and HAR are reevaluated and updated annually.

Figure 9-1 does not provide a schedule for the initial safety assessment as the figure addresses only Part B activities. The initial safety assessment package was delivered to the Regulatory Unit in December 1997 as part of the Part A activities (BNFL 1997c).

9.3 Flow of Safety-Related Work and Deliverables

Figure 9-1 shows the interdependencies between the deliverables.

The scope of the proposed Limited Work Authorization (LWA) included in Figure 9-1 provides for early initiation of construction activities. The LWA allows for excavation, backfill, recompaction, and installation of the mud mat and ground grid. The LWA request would include information on site suitability (addressing hazards from natural phenomena and nearby facilities as they would impact the requested construction activity); excavation, backfill, and recompaction criteria; stability of surface soils; design requirements and Quality Assurance Program to be applied to the requested LWA activities; current SRD standards and ISMP program applicable to LWA activities; description of planned safety-related testing to be performed during LWA activities; references to the procedures to be employed for the requested work; and the environmental impacts of implementing the requested work activity.

10.0 Assessments

Assessments of the Project verify that public and worker safety considerations are reflected in the design, procurement, construction, commissioning, operation, and deactivation of the facility. The role of safety committees in achieving these objectives is discussed in Integrated Safety Management Plan (ISMP) Section 3.16.1, "Safety Committees".

Assessments in compliance with 10 CFR 830.120(c)(3)(i) and (c)(3)(ii) involve the following:

1) Management assessments. Managers assess their management processes so that problems that hinder the organization from achieving its objectives are identified and corrected. These assessments are discussed in Section 10.1, "Management Assessments".
2) Independent assessments. Independent assessments are performed to measure item and service quality, measure the adequacy of work performance, and promote improvement. These assessments are discussed in Section 10.2, "Independent Assessments".

During the design and construction phase, assessments are directed at such activities as:

1) The development of regulatory documents
2) Performance of safety analysis
3) Qualification of personnel, training, and procedures as related to design and construction
4) Design control
5) Construction work packages
6) Worker safety
7) Fire protection
8) Equipment procurement.

Assessments during operation and deactivation provide oversight of these same areas and extend to the following areas:

1) Radiation control
2) Unreviewed safety questions evaluations
3) Compliance with the authorization basis
4) Maintenance training and work performance
5) Hazardous waste management
6) Emergency exercises
7) Compliance to deactivation end point criteria
8) Fire protection.

The following sections provide a summary of the more significant aspects of the assessment processes.

10.1 Management Assessments

Management assessments are conducted annually by the line manager of each RPP-WTP organization to measure the effectiveness of their activities in achieving public and worker safety. The assessments focus on the various functional programs for which managers have safety responsibility.

The assessments cover, but are not limited to the following:

1) Interfaces among groups with safety roles
2) Use of safety performance indicators
3) Adequacy of resources
4) Staff training and qualification
5) Supervisory oversight and support.

Management assessments involve the following:

1) Evaluating the implementation of applicable portions of the quality assurance program
2) Identifying barriers hindering the accomplishment of safety objectives, documenting response actions, and implementing corrective actions
3) Developing a plan for each management assessment that includes the schedule, scope, level of effort, and team qualifications
4) Issuing a final report with identification of problems and corrective actions
5) Evaluating the effectiveness of the corrective actions in preventing recurrences.

Section 18 of the QAM addresses the purpose and conduct of management assessments and specific managers' responsibilities in the assessment process.

10.2 Independent Assessments

Independent assessments measure the effectiveness of activities in achieving public and worker safety. The staff performing independent assessments have sufficient authority and freedom outside the line organization to carry out their responsibilities. Individuals performing independent assessments are technically qualified and knowledgeable in the areas being assessed. Independent assessments are performed to identify the following:

1) Work performance and process effectiveness
2) Abnormal performance and potential problems
3) Improvement opportunities
4) Effectiveness of root cause identification and corrective actions in preventing recurrence of previous problems
5) Lessons learned from other organizations with similar activities or concerns.

The frequency of the assessments for various functional areas is based on the following:

1) Status, complexity, and importance of the activity or process being assessed
2) Past performance of the activity or process being assessed
3) Performance indicator results and trending to ensure activities are achieving adequate public and worker safety.

Section 8 of the QAM addresses the purpose and conduct of independent assessments, independence and qualifications of assessment personnel, documentation of results, management responses and actions, and specific managers' responsibilities in the assessment process.

10.3 Corrective Action Implementation and Tracking

An administrative system is established for tracking corrective action items. Problems are evaluated and trended to determine if any should be reported in an incident report or reported under 10 CFR 820, "Procedure Rules for DOE Nuclear Facilities" as a significant noncompliance with a nuclear safety requirement. Effectiveness of the corrective actions in preventing recurrence of previous problems is evaluated in a subsequent management assessment.

10.4 Support of DOE Inspection and Corrective Action/Enforcement Action Programs

This section addresses the DOE inspection and corrective active/enforcement action programs including the Project's responsibilities relative to these programs.

10.4.1 DOE Inspection Program

The DOE inspection program is described in *Inspection Program Description for the Regulatory Oversight of TWRS Privatization Contractors,* (DOE-RL 1998b). The purposes of this inspection program are described as:

1) Confirming Contractor performance to the authorization basis and Contract in the areas of radiological, nuclear, and process safety
2) Ensuring timely identification and implementation of corrective actions such that regulatory conditions detrimental to safety and the interests of fixed-price contracting are avoided
3) Developing independent inputs for subsequent regulatory authorization or actions thereby fostering regulatory efficiency.

The DOE inspection program is executed in a planned, disciplined, and predicable manner. This is accomplished through appropriate planning, preparation, and performance of inspections and through the use of established protocols (DOE-RL 1998b).

The Project supports the DOE inspection program by:

1) Making available for DOE review, documentation such as program plans, manuals, procedures, instructions, technical reports, self-assessment reports, meeting minutes, records, data reports and event reports
2) Providing briefings and discussions and support interviews on selected subjects as requested by the DOE and prearranged with BNI.
3) Supporting on-location DOE observations of Project operations and activities as requested by the DOE and prearranged with BNI.
4) Supporting unannounced on-location DOE observation of Project construction, operation, and deactivation activities
5) Attending and supporting pre-inspection and inspection entrance and exit meetings
6) Responding to findings of DOE inspection activities.

The above-mentioned RPP-WTP operations and activities to be observed include, but are not limited to, 1) monitoring of equipment performance during operation, inspection, or testing, 2) witnessing of tests, and 3) the performance of independent analyses.

10.4.2 DOE Corrective Action/Enforcement Action Program

The DOE corrective action/enforcement actions program is described in *Corrective Action/Enforcement Action Program Descriptions* (DOE-RL 1998a). The Project supports the DOE corrective action and enforcement actions program by:

1) Self-identification of non-compliant conditions and the prompt reporting of such conditions to DOE
2) Responding to corrective action notices issued by DOE
3) Prompt implementation of a safety-rework, suspend operation, stop work, and Compliance Orders issued by the DOE.

11.0 Organization Roles, Responsibilities, and Authorities

The responsibility for the design, construction, commissioning, operation, and deactivation of the River Protection Project-Waste Treatment Plant lies with the designated RPP-WTP contractors throughout these various life-cycle phases of the Facility. These contractors to the Department of Energy, Office of River Protection will include the Design, Construction, and Commissioning (DC&C) contractor, the Operations contractor, and the Deactivation contractor.

As addressed in this ISMP, these contractor's roles, responsibilities, and authorities include defining and implementing nuclear, radiological, and process safety standards and the related safety bases for protection of the RPP-WTP occupational workers and the public. These RPP-WTP contractors have the sole responsibility for defining and implementing DOE-approved safety standards and communicating those safety standards as requirements to all RPP-WTP Project team members and subcontractors who conduct work on the Project.

While the Project team members manage subcontractors, the RPP-WTP contractors retain responsibility for oversight of team members and subcontractors performance and for overall project safety. The commitment inherent in this structure is that line management retains the responsibility for development and implementation of the safety basis. Although some specific roles may be reassigned within the organization, line management's responsibility for safety is invariant.

The RPP-WTP contractors assign safety roles to functional areas as indicated in Tables 9-1 through 9-5. Table 9-1 assigns roles for key elements of the design phase functional groups. The organization chart for the DC&C contractor organization is provided in Figure 11-1. The Operations and Deactivation contractors organization charts will be defined as the Project nears these phases of the Project. Project roles, responsibilities, and authorities for the DC&C contractor are presented in Section 11.1. Envisioned roles, responsibilities, and authorities for the Operations contractor are presented in Section 11.2.

11.1 Design, Construction, and Commissioning Contractor Organization Roles, Responsibilities, and Authorities

Safety-related roles, responsibilities, and authorities for the DC&C phase of the operation, as assigned to individuals and organizations within BNI (the DC&C Contractor), are discussed below.

Project Manager

The Project Manager safety-related roles, responsibilities, and authorities include:

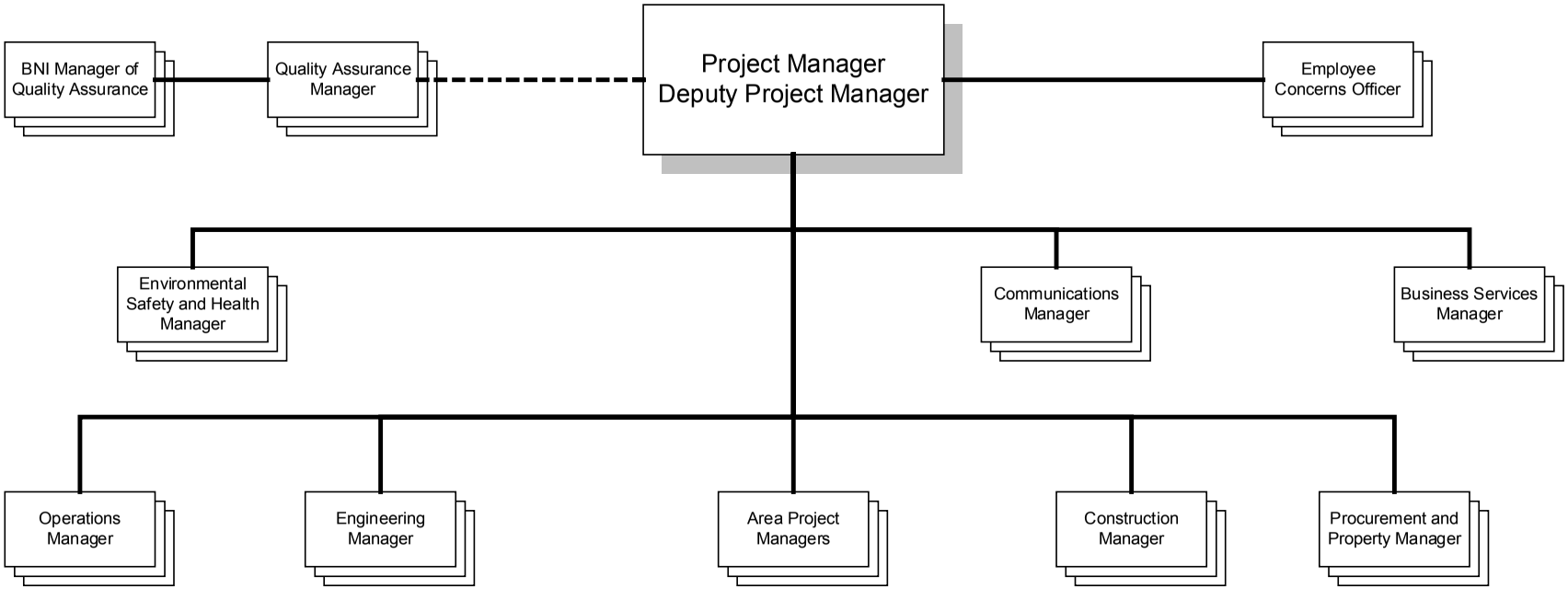
1) Responsibility for RPP-WTP safety
2) Defining safety policy, objectives, and interfaces
3) Assigning roles and responsibilities for safety-related activities
4) Setting performance expectations
5) Developing management assessment policies
6) Signatory on permit applications for construction of the Facility
7) Serving as a member of the Executive Committee
8) Ensuring implementation of the Quality Assurance Program (QAP)

Deputy Project Manager

The Deputy Project Manager safety-related roles, responsibilities, and authorities include:

1) Ensuring that the RPP-WTP is designed, constructed, tested, commissioned, operated, and maintained in a safe, reliable, and efficient manner in accordance with policies and all applicable laws, regulations, authorization bases, and technical requirements
2) Integrating nuclear and industrial safety, quality, and environmental protection into all work
3) Managing the design transition, facility and process design, construction, acceptance testing, commissioning, procurement, and operations
4) Integrating the Area Project Managers and functional managers
5) Creating an atmosphere in the workplace where reporting and resolution of conditions adverse to quality is encouraged at all levels
6) Stopping activities within his area of responsibility, which are not accomplished in compliance with applicable authorization bases and/or regulatory requirements

Figure 11-1 Management Structure and Organization for the BNI Design, Construction, and Commissioning Contract



Area Project Managers

The safety-related roles, responsibilities, and authorities of the Area Project Managers, in their respective areas of responsibility, include:

1) Managing design and construction effort, in their respective area of responsibility.
2) Implementing management assessment policies, in their respective area of responsibility.
3) Implementing the contractor requirements of 10 CFR 820, "Procedural Rules for DOE Nuclear Activities", in their respective area of responsibility.
4) Ensuring the development and implementation of the incident reporting program, in their respective area of responsibility.
5) Ensuring approval by the Engineering Manager of final designs of Safety Design Class and Safety Design Significant features, in their respective area of responsibility.
6) Serving as principal interface with DOE on technical issues, in their respective area of responsibility.
7) Developing and managing the readiness review program to support commissioning, in their respective area of responsibility.

Engineering Manager

The Engineer Manager oversees the engineering design activities that are assigned to the DC&C contractor. The safety-related roles, responsibilities, and authorities of the Engineering Manager include:

1) Approving final designs of Safety Design Class and Safety Design Significant features
2) Updating the treatment process, civil, architectural, structural, electrical, and mechanical design criteria
3) Completing the civil, structural, support system, and facility designs including the incorporation of regulatory and quality commitments
4) Preparing specifications for procurement of pre-purchased equipment
5) Incorporating regulatory and quality commitments into the design, procurement, fabrication, inspection, and testing of systems and components
6) Designing measures to facilitate performance of Technical Safety Requirement (TSR) surveillances
7) Designing features to implement the design requirements of 10 CFR 835 Occupational Radiation Protection including features for ensuring personnel exposure during operation is as low as reasonably achievable (ALARA)
8) Selecting materials for fabrication and construction; defining methods for corrosion control; and specifying welding procedures, requirements for nondestructive examination, and codes and standards
9) Designing fire prevention, detection, and suppression features in compliance with state and federal requirements
10) Incorporating deactivation and decommissioning features into the facility design
11) Evaluating proposed changes to civil, structural, support system, and facility designs
12) Updating the process design specifications, process descriptions, basis of design documents
13) Completing the process design including the incorporation of regulatory and quality commitments

14) Developing and implementing the configuration management (CM) program to control the safety and design bases
15) Obtaining documentation defining the physical configuration of the facility and forwarding this documentation to the Project Administration and Controls Organization
16) Developing and implementing of CM program database

Construction Manager

The safety-related roles, responsibilities, and authorities of the Construction Manager include:

1) Implementing procedures and training to enhance construction safety
2) Providing input to the configuration management program including as-built information
3) Supporting the incident reporting system for construction-related incidents
4) Developing procedures for the handling of hazardous material during construction, including packaging, labeling, storage, and shipping practices
5) The packaging and manifesting of dangerous waste arising from construction activities
6) Interfacing with subcontractors on process safety management and ES&H matters
7) Incorporating regulatory and quality commitments of SSCs into the construction
8) Implementing the construction testing program to verify that SSCs meet acceptance testing requirements

Environment, Safety & Health (ES&H) Manager

The safety-related roles, responsibilities, and authorities of the ES&H Manager include:

1) Implementing internal safety and oversight functions
2) Developing safety basis and safety-related performance measures
3) Implementing the process safety management program
4) Developing and implementing the regulatory commitment tracking system, and the incident reporting program
5) Interfacing with regulators, stakeholders, and Hanford Site contractors on ES&H matters
6) Evaluating proposed changes that involve implementation of nuclear, radiological, and process safety and environmental matters
7) Implementing the fire protection program
8) Coordinating cooperative agreements with outside agencies such as fire, police, ambulance, and medical services
9) Developing and managing the ES&H portions of the readiness review program to support commissioning
10) Serving as a member of the Project Safety Committee, supporting independent safety review in the ES&H area of responsibility and serving as the PSC alternate chairperson.
11) Updating the process hazards analysis

The ES&H Manager also oversees activities related to radiological, nuclear, and process safety and environment protection. These activities include the following:

1) Identifying and evaluating new laws and regulations that may affect the Project safety programs
2) Preparing the Limited Construction Authorization (LCA) request
3) Interfacing with the regulators during onsite inspections
4) Updating the Hazard Analysis Report (HAR), Safety Requirements Document (SRD), and Integrated Safety Management Plan (ISMP)
5) Preparing the Preliminary Safety Analysis Report (PSAR) and Final Safety Analysis Report (FSAR)
6) Environmental reporting
7) Identifying requirements for worker and public safety, security, and environmental regulatory compliance
8) Preparing the environmental characterization and monitoring plans
9) Preparing permit applications and plans as required for state and federal environmental regulations
10) Monitoring environmental compliance during construction
11) Developing and implementing the Environmental Radiation Protection Program

Quality Assurance Manager

The safety-related roles, responsibilities, and authorities of the QA Manager the following:

1) Developing the Quality Assurance Program (QAP)
2) Assessing and auditing project activities to verify compliance with the QAP and other requirements and to determine the effectiveness of the QAP
3) Providing support for the development of qualification and training programs to ensure that required capabilities are achieved and maintained by project personnel
4) Reviewing project documents (e.g., design documents, nuclear and process safety deliverables, work plans, and source evaluation plans) to verify inclusion of appropriate QAP requirements
5) Recommending and exercising work stoppage or controls over further processing in response to quality concerns
6) Assessing and auditing vendor and subcontractor activities to verify compliance with the QAP and other requirements and to determine the effectiveness of the QAP
7) Serving as a member of the Project Safety Committee, supporting independent safety review in the QA area of responsibility

The QA Manager has the authority and responsibility to stop project work when the work, if allowed to continue, would result in activities or documents being in noncompliance with stated QAP requirements. The QA Manager is responsible for determining when appropriate corrective or preventative actions have been taken and for lifting the stop work order to allow work to proceed.

Operations Manager

The safety-related roles, responsibilities, and authorities of the Operations Manager include:

1) Developing a program for operations procedure preparation, review, verification, validation, approval, change, deviation, and internal control
2) Writing and maintaining operating procedures including post-deactivation activities
3) Performing administrative responsibilities including maintaining a qualified staff and ensuring effective employee performance
4) Performing radioactive commissioning testing to demonstrate compliance with the acceptance criteria and documenting the results to acceptance criteria.
5) Serving as the chairperson for the Project Safety Committee
6) Developing and managing the readiness review program to support commissioning

Research and Technology Manager

The safety-related roles, responsibilities, and authorities of the Research and Technology (R&T) Manager include:

1) Serving as a member of the Project Safety Committee, supporting independent safety review in the R&T area of responsibility.

Process Technology Manager

The safety-related roles, responsibilities, and authorities of the Process Technology Manager include:

1) Ensuring that technologies are developed and demonstrated
2) Evaluating the completed process design and proposed changes to the design
3) Identifying commissioning tests to be performed and their acceptance criteria
4) Incorporating regulatory and quality commitments into procurement, fabrication, inspection, and testing of process components
5) Performing systematic design reviews to determine readiness to authorize fabrication and construction of structures, systems, and components (SSC)
6) Implementing design considerations for deactivation and decommissioning

Commissioning Manager

The commissioning organization manages the commissioning program. The safety-related roles, responsibilities, and authorities of the Commissioning Manager include:

1) Developing the objectives and scope for the startup program
2) Developing and evaluating proposed changes to the commissioning program
3) Verifying and validating operation and maintenance procedures during performance of testing

4) Providing information from the startup program to the operations, training, and procedures groups, and maintenance for verification and validation of operating administrative controls

Procurement and Property Manager

The Procurement and Property Manager safety-related roles, responsibilities, and authorities include:

1) Providing the processes and procedures for procuring items and services important to safety.
2) Providing full support to the Quality Assurance Program described in the *Quality Assurance Manual* (QAM), thereby assuring that all work performed under his cognizance will conform to and support the requirements of the QAM.

Business Services Manager

The safety-related roles, responsibilities, and authorities of the Business Services Manager include:

1) Implementing an employee feedback program
2) Controlling the facility policy manual (containing the Project Manager safety policy) and all procedures
3) Developing and maintaining the records management program (See Table 8-1)

11.2 Operations Contractor Organization Roles, Responsibilities, and Authorities

The envisioned safety-related roles, responsibilities, and authorities for the Operations phase of the operation, as assigned to individuals and organizations within the Operations Contract, are discussed below.

Facility Manager

Responsibilities and roles of the Facility Manager include the following:

1) Ensuring the development and implementation of facility controls to protect the health and safety of the public, and workers and to protect the environment from hazardous situations associated with the chemical and radiological hazards of the facility
2) Ensuring that operational activities are properly staffed and controlled
3) Managing operation of the facility to obtain the defined work activity while maintaining the authorization basis for the facility
4) Approving Facility activities, including modifications to Safety Design Class and Safety Design Significant SSCs
5) Ensuring that work is performed in conformance with procedures, policies, and safety requirements

6) Implementing the contractor requirements of 10 CFR 820, "Procedural Rules for DOE Nuclear Activities"
7) Serving as the Emergency Director during events categorized as emergencies
8) Assigning roles and responsibilities for activities related to safety including operations, performance improvements, safety improvements, and deactivation of the facility

Operations Manager

Roles of the Operations Manager include the following:

1) Developing a program for procedure preparation, review, verification, validation, approval, change, deviation, and internal control
2) Writing and maintaining operating procedures including post-deactivation activities
3) Performing administrative responsibilities including maintaining a qualified staff and ensuring effective employee performance
4) Performing radioactive startup testing to demonstrate compliance with the acceptance criteria and documenting the results to acceptance criteria
5) Managing daily facility operation to obtain the define work activity while maintaining compliance to the TSRs
6) Performing TSR surveillances assigned to operations and supporting those TSR surveillances assigned to the Maintenance Organization
7) Scheduling and managing process system outage activities
8) Initiating and managing deactivation
9) Obtaining an understanding of the features and limitations of the facility SSCs to facilitate radioactive startup testing, facility operation, and the development of procedures and training
10) Developing and implementing the operating staff training program
11) Writing and evaluating proposed changes to administrative procedures related to facility operation
12) Ensuring operation of support systems (e.g., electrical, instrument air, and steam)
13) Performing analysis of feed material, product, and process chemicals
14) Developing procedures for hazardous material handling, packaging, labeling, storage, and shipping practices
15) The packaging and manifesting of dangerous waste
16) Evaluating proposed changes to the radioactive startup program

Environment, Safety, & Health Manager

The ES&H Manager is a member of the PSC and serves as the PSC alternate chairperson. In addition, for the operating project the ES&H organization has the following roles:

1) Developing the emergency plan and the emergency plan implementing procedures
2) Managing emergency drills and exercises
3) Modifying plans and procedures to address internal safety and oversight functions for the deactivation phase
4) Developing deactivation safety performance measures, modification of plans and procedures, and confirmation the facility meets the safe storage criteria on completion of deactivation
5) Managing occupational health and safety
6) Obtaining monitoring, sampling, and record keeping information on facility discharges
7) Maintaining state and federal environmental permits

8) Maintaining the environmental database
9) Keeping environmental regulators informed on current status, concerns, and new data
10) Identifying critical aspects of facility deactivation that would affect environmental regulatory compliance
11) Developing the USQ identification and evaluation process
12) Developing TSR surveillance testing and evaluation program
13) Monitoring compliance to the authorization basis
14) Updating authorization basis documentation including the FSAR
15) Directing incident investigations including reporting, root cause analyses, identification of corrective actions, and tracking of effectiveness of corrective actions and applying lessons learned from relevant facilities
16) Developing a process for evaluating deficiencies to nuclear safety requirements subject to 10 CFR 820, "Procedural Rules for DOE Nuclear Activities"
17) Preparing a deactivation safety analysis report
18) Developing and implementing the Radiation Protection Program for operations that is compliant with 10 CFR 835, "Occupational Radiation Protection"
19) Performing radiation and contamination surveys and maintaining personnel exposure records
20) Informing management of conditions that could lead to exceeding radiation limits established for radiation areas or exceeding administrative limits for personnel radiological exposure
21) Monitoring deactivation activities to ensure personnel exposure meets as low as reasonably achievable (ALARA) objectives

Quality Assurance Manager

The QA Manager is a member of the PSC. Roles of the QA Organization include the following:

1) Establishing a Quality Assurance Program for operations
2) Performing independent assessments and program compliance audits
3) Reviewing the project quality procedures and documenting compliance with applicable QAP requirements
4) Modifying and implementing quality assurance plans and procedures for the for deactivation process
5) Verifying implementation of corrective action measures and determining that the solutions for quality problems are effective

The QA Manager has the authority and responsibility to stop project work when the work, if allowed to continue, would result in activities or documents being in noncompliance with stated requirements. The QA Manager is responsible for determining when appropriate corrective or preventative actions have been taken and for lifting the stop work order to allow work to proceed.

Engineering Manager

The Engineering Manager a member of the PSC. Roles of the Engineering organization include the following:

1) Evaluating startup test results and comparing the results to acceptance criteria
2) Developing and evaluating proposed design improvements and changes to engineered features
3) Supporting resolution of production problems
4) Developing the surveillance and maintenance criteria for facility operations
5) Identifying measures that minimize hazards associated with treating and storing radioactive waste, and for the safe handling of fissionable materials
6) Performing a job hazard analysis and participating with ES&H to update HAR
7) Updating the process hazards analysis (PHA) to support permit and authorization basis updates
8) Preparing and implementing a deactivation management plan that includes:
   - updating the HAR
   - defining surveillance and maintenance criteria for deactivation and safe storage
   - developing facility modifications to facilitate performance of surveillance tests
   - implementing measures that minimize hazards associated with treating and storing radioactive materials

Maintenance Manager

The Maintenance Manager oversees the activities of the Maintenance organization. Roles of the Maintenance organization include:

1) Defining and implementing a maintenance program that includes preventive, predictive, and corrective maintenance practices and incorporates vendor-recommended maintenance activities and equipment history
2) Performing TSR surveillances assigned to maintenance and supporting those TSR surveillances assigned to operations
3) Implementing facility modifications
4) Developing and modifying operating and maintenance instructions for post-deactivation operational equipment
5) Writing maintenance procedures
6) Collecting and processing baseline data for system and component performance monitoring and maintenance planning

Procurement and Property Manager

The Procurement and Property Manager's safety related roles, responsibilities, and authorities include:

1) Providing the processes and procedures for procuring items and services important to safety.
2) Providing full support to the Quality Assurance Program described in the *Quality Assurance Manual* (QAM), thereby assuring that all work performed under his or her cognizance will conform to and support the requirements of the QAM.

Startup Manager

The Startup organization manages the startup testing program. Additional roles of the Startup Manager include the following:

1) Evaluating proposed changes to the startup program
2) Verifying and validating operation and maintenance procedures during performance of testing
3) Providing information from the startup program to the operations, training, and procedures groups, and maintenance for verification and validation of operating administrative controls

Configuration Management Manager

The Configuration Management Manager oversees the activities of the Configuration Management organization. Roles of the Configuration Management organization include the following:

1) Continued implementation of the operational configuration management program
2) Maintaining the facility operating history to facilitate deactivation of the facility

Administration and Controls Manager

The Administration and Controls Manager continues those activities started by the DC&C contractor Business and Project Controls Organization

12.0 Definitions

In the following list, the parenthetical information following the term being defined is the source of the definition. However, for sources other than DOE/RL-96-0006 (DOE 1996b) or the BNFL Inc./DOE contract (DOE-RL 1996c), the wording provided may be tailored to the Project use and therefore may not be exactly as contained in the referenced source.

Accident Risk Goal (DOE/RL-96-0006 [DOE-RL 1996b]). The risk, to an average individual in the vicinity of the Contractor's facility, of prompt fatalities that might result from an accident should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population generally are exposed.

By footnote 14 of DOE/RL-96-0006, for evaluation purposes, individuals are assumed to be located within 1 mile of the contractor's controlled area.

Acute Hazard (AIChE 1992). The potential for injury or damage to occur as a result of an instantaneous or short duration exposure to the effects of an accident.

Administrative Controls. Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of the facility.

As Low as Reasonably Achievable (10 CFR 835). The approach to radiation protection to manage and control exposures (both individual and collective) to the work force and to the general public to as low as is reasonable, taking into account social, technical, economic, practical, and public policy considerations. The ALARA approach is not a dose limit but a process that has the objective of attaining doses as far below the applicable limits of this part (10 CFR 835) as is reasonably achievable.

Authorization Basis (DOE/RL-96-0006 [DOE-RL 1996b]). The composite of information provided by a Contractor in response to radiological, nuclear, and process safety requirements that is the basis on which the Director of the Regulatory Unit grants permission to perform regulated activities.

Changes (RL/REG-97-13). Changes to the facility design and administrative controls that are described in the authorization basis or are relied upon by the Contractor to ensure conformance to the authorization basis. Included within the scope of "Changes" are those items that may not be explicitly described in the authorization basis, but where Changes would cause a deviation from commitments contained in the authorization basis.

As used above, "facility" refers to the physical facility, the hazards and safety analysis of the facility, and the work at the facility that is enveloped by the analyses. The facility is described in the authorization basis by information such as: the site description, design information, hazard analysis information, safety analysis information, and descriptions of facility operations, tests, and experiments.

As used above, "administrative controls" refers broadly to the management and administrative processes associated with managing, designing, building, or operating the facility. Administrative controls are described in the authorization basis by information such as the descriptions of procedures, programs, plans, and management processes.

Codes and Standards. Document containing expressed expectations for the performance of work; normally refers to those practices issued by consensus organizations (e.g., American National Standards Institute, American Society of Mechanical Engineers, and National Fire Protection).

Co-located Worker (DOE/RL-96-0006 [DOE-RL 1996b]). An individual within the Hanford Site, beyond the Contractor-controlled area, performing work for or in conjunction with DOE or utilizing other Hanford Site facilities.

Common-Cause Failures (DOE/RL-96-0006 [DOE-RL 1996b]). Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures.

Common-Mode Failures (DOE/RL-96-0006 [DOE-RL 1996b]). Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation.

Consequence (AIChE 1992). The direct, undesirable result of an accident sequence usually involving a fire, explosion, or release of toxic material. Consequence descriptions may be qualitative or quantitative estimates of the effects of an accident in terms of factors such as radiological exposure, health impacts, economic loss, and environmental damage.

Consequence Analysis (AIChE 1992). The analysis of the effects of incident outcome cases independent of frequency or probability.

Controlled Area (DOE/RL-96-0006 [DOE-RL 1996b]). The physical area enclosing the facility by a common perimeter (security fence). Access to this area can be controlled by the contractor. The controlled area may include identified restricted areas.

Deactivation (Contract, Section J, Attachment 9 [DOE-RL 1996c]). The process of permanently ceasing active operation at a facility in a planned and controlled manner to support follow-on decontamination and decommissioning activities. A process whereby non-essential systems and/or equipment in a shut down facility are de-energized, drained and flushed, isolated, or removed to minimize the long-term costs of maintaining the facility in a physically safe and environmentally secure condition. Includes the removal of fuel and stored radioactive and/or hazardous waste from the facility and implementation of appropriate facility safety requirements.

Deterministic Analysis. A non-probabilistic approach to accident analysis that begins with the establishment of a specific set of credible accident initiating events expected to represent a range of possible challenges to the safety of the facility and some of which are expected to define the design requirements for the facility. The design of the facility is then evaluated to this set of events using conservative inputs and assumptions to account for uncertainties, to ensure that adequate controls exist to protect the public and workers such that radiological and chemical exposure standards are satisfied. In the evaluation of public and worker safety, the most limiting random single active failure of a system or component is assumed and credit is taken only for those structures, systems, and components that meet Safety Design Class requirements. Other than selecting credible events to account for accident likelihood, this is a consequence-oriented rule-followed approach (i.e., assume worst single failure) to establish the design of the facility.

Regulatory Unit (DOE/RL-96-0006 [DOE-RL 1996b]). The organization reporting to the Director of the Regulatory Unit dedicated to supporting the Director in executing regulatory authority.

Double-shell Tank (Contract, Section J, Attachment 9 [DOE-RL 1996c]). A reinforced concrete underground vessel with two inner steel liners to provide containment and backup containment of liquid wastes; annulus is instrumented to permit detection of leaks from the inner liner. At the Hanford Site, there are 28 double-shell tanks.

Emergency Response Planning Guidelines (AIChE 1992). A system of guidelines for airborne concentrations of toxic materials prepared by the American Industrial Hygiene Association (AIHA).

Engineered Feature. A structure, system, or component that contributes to the safe operation of the facility.

Episodic Event (AIChE 1992). An unplanned event of limited duration, usually associated with an accident.

ERPG-2 (AIHA 1988). The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair their abilities to take protective action.

External Event. An event external to the RPP-WTP caused by (1) a natural hazard (e.g., earthquake, flood, lightning, or range fire) or (2) a human-induced event (e.g., transportation or nearby industrial activity).

Facility Worker. An individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities. This is the same as the definition of 'worker' in DOE/RL-96-0006 which is "Worker means an individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities".

Final Safety Evaluation Report (DOE/RL-96-0006 [DOE-RL 1996b]). The document approved and issued by the Director of the Regulatory Unit that addresses the adequacy of the authorization basis for operation.

Graded Approach (10 CFR 830.3). A process by which the level of analysis, documentation, and actions necessary to comply with a requirement in this part (i.e., 10 CFR Part 830) are commensurate with:

1) Relative importance to safety, safeguards, and security
2) Magnitude of any hazard involved
3) Life cycle stage of a facility
4) Programmatic mission of a facility
5) Particular characteristics of a facility
6) Any other relevant factor

Hanford Site. A 1,450 km^2 reservation in southeast Washington State owned by the Federal Government. Established in 1943 as part of the Manhattan Project, the initial activity on the Hanford Site was to produce plutonium for use in nuclear weapons for the nation's defense. The Hanford Site has had nine production reactors and four chemical separation plants. The current mission on the Hanford Site is environmental cleanup and development of related technologies.

Hazard (DOE/RL-96-0006 [DOE-RL 1996b]). A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel, damage to an operation, or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).

Hazard and Operability Analysis (AIChE 1992). A systemic method in which process hazards and potential operating problems are identified using a series of guide words to investigate process deviations.

Hazardous Material. A solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health.

High-Level Waste (Contract, Section J, Attachment 9 [DOE-RL 1996c]). The highly radioactive waste material that results from the operation of the first-cycle solvent extraction system or equivalent and subsequent extraction cycles or equivalent that contains a combination of transuranic waste and fission products in concentrations requiring permanent isolation.

High Radiation Area (10 CFR 835). Any area, accessible to individuals, in which radiation levels could result in an individual receiving a deep dose equivalent in excess of 0.1 rem (0.001 sievert) in 1 hour at 30 centimeters from the radiation source or from any surface that the radiation penetrates.

Highly Hazardous Chemical (DOE/RL-96-0006 [DOE-RL 1996b]). A substance possessing toxic, reactive, flammable, or explosive properties as defined by 29 CFR 1910.119.

Human Factors (AIChE 1992). A discipline concerned with designing machines, operations, and work environments to match human capabilities, limitations, and needs. Among human factors specialists, this general term includes any technical work (engineering, procedure writing, worker training, worker selection) related to the person in operator-machine systems.

Important-to-Safety (DOE/RL-96-0006 [DOE-RL 1996b]). Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction (i.e., support systems, subsystems, or components). Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety (i.e., safety-related may be practical). However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Independent Safety Review Team. A group of individuals with the demonstrated knowledge and expertise to confirm the completeness, credibility, and adequacy of the Project radiological, nuclear, process safety documents, and recommend their approval to the Project Manager.

Initial Safety Evaluation Report (DOE/RL-96-0006 [DOE-RL 1996b]). The document, approved and issued by the Director of the Regulatory Unit, that addresses the capability or potential for obtaining future authorizations for construction, operation, and deactivation.

Initiating Event (AIChE 1992). The first event in an event sequence. Can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident.

Internal Event. An occurrence related to structure, system, and component performance or human action, or an occurrence external to the system but within the RPP-WTP that causes upset of a structure, system, or component.

Likelihood (AIChE 1992). A measure of the expected probability or frequency of an event's occurrence.

Limiting Conditions for Operations (DOE/RL-96-0006 [DOE-RL 1996b]). The lowest functional capability or performance level of equipment required for safe operation of the facility.

Low-Activity Waste (Contract, Section J, Attachment 9 [DOE-RL 1996c]). Low-level tank waste that has not yet received NRC concurrence as incidental.

Margin of Safety (DOE/RL-96-0006 [DOE-RL 1996b]). The level of confidence that is assigned to the integrity of radiological control measures such as confinement barriers. It is defined as the range between the design acceptance limits and the design failure point of the control feature. The design acceptance limits for radiological control measures such as confinement barriers are established during the design of the facility. These criteria are given in terms of those physical parameters that define their performance. Whenever the values of the design acceptance limits are exceeded, the margin of safety, and therefore the confidence in the integrity of the control feature, is decreased.

Major Accident. Relative to implementation of the incident investigation and reporting requirements of 29 CFR 1910.119(m), a major accident is a major uncontrolled emission, fire, or explosion, involving one or more highly hazardous chemicals or radioactive materials, that presents serious danger to facility workers.

Mitigative Feature. A structure, system, component, or administrative control that serves to reduce the consequences of a hazardous situation or accident.

Normal Operation (DOE/RL-96-0006 [DOE-RL 1996b]). Steady-state operation and those departures from steady-state operation that are expected frequently or regularly in the course of facility operation, system testing, and maintenance. It includes conditions such as startup, shutdown, standby, anticipated operational occurrences, operation with specific equipment out of service as permitted by the approved operational constraints, and routine inspection, testing, and maintenance of components and systems during any of these conditions if it is consistent with the approved operational constraints.

Operations Risk Goal (DOE/RL-96-0006 [DOE-RL 1996b]). The risk, to the population (public and workers) in the area of the Contractor's facility, of cancer fatalities that might result from facility operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks to which members of the U.S. population generally are exposed.

By Footnote 13 to DOE/RL-09-0006, for evaluation purposes, individuals are assumed to be located within 10 miles of the controlled area.

Preventative Feature. A structure, system, component, or administrative control that serves to preclude the occurrence of a hazardous situation or accident.

Probabilistic Analysis. An approach to accident analysis that addresses all credible initiating events and that is risk-based in that it considers both the likelihood and consequences of accidents to determine overall risks. Mitigating system and component reliability as well as human performance are assessed probabilistically to support risk-informed decision making. The probabilistic analysis goes beyond the single failure requirements of the deterministic approach in that it assesses the probabilities of multiple failures. This is a "best-estimate" analysis in that realistic input and modeling assumptions are used and all of the available structures, systems, and components are considered that can prevent or mitigate the event. The evaluation of the availability and reliability of structures, systems, and components considers failure to start and failure to run as well as maintenance-caused unavailabilities.

Process (DOE/RL-96-0006 [DOE-RL 1996b]). Any activity involving a highly hazardous chemical including use, storage, manufacturing, handling, or the onsite movement of such chemicals, or a combination of these activities.

Process Hazards Analysis. The identification of hazards and the analysis of the significance of hazardous situations associated with a process or activity. It includes preliminary hazard analysis and Hazard and Operability Analysis (HAZOP).

Process Safety DOE/RL-96-0006 [DOE-RL 1996b]). The operation of facilities that handle, use, process, or store hazardous materials in a manner free of episodic or catastrophic incidents. However, the handling, use, processing, and storage of materials with inherent hazardous properties can never be done in the total absence of risk. Process safety is an ideal condition towards which one strives.

Process Safety Management DOE/RL-96-0006 [DOE-RL 1996b]). The application of management systems to the identification, understanding, and control of process hazards to prevent process-related injuries and incidents.

Public DOE/RL-96-0006 [DOE-RL 1996b]). Individuals who are not occupationally engaged at the Hanford Site.

Radiation Exposure. Radiation exposure, as used in Project documents, is the exposure of people (public, facility workers, collocated workers) to ionizing radiation produced by radioactive material. Unless otherwise specified, radiation exposure means the total effective dose equivalent (TEDE), that is, the sum of external and internal exposures. External exposures are assessed as the resulting effective dose equivalent; internal exposures as the resulting committed effective dose equivalent. Other terms used in Project documents, such as radiological exposure, dose, radiation dose, and the like, are taken as synonymous to radiation exposure.

Radiological, Nuclear, and Process Safety (Contract, Section J, Attachment 9 [DOE-RL 1996c]). Those actions taken to control the hazards incident to possession, use and disposal of radioactive and nuclear material, and the processing of hazardous chemicals.

Radiological Worker (10 CFR 835). A general employee whose job assignment involves operation of radiation-producing devices, or working with radioactive materials, or who is likely to be routinely occupationally exposed above 0.1 rem (0.001 sievert) per year total effective dose equivalent (TEDE).

Regulatory Guides. Documents that describe methods acceptable to the U.S. Nuclear Regulatory Commission (NRC) staff for implementing specific portions of NRC regulations. Some regulatory guides lay out steps taken by the staff in evaluating specific situations. Others provide guidance to applicants concerning information needed by staff in its review of applications for permits and licenses, or refer to or endorse national standards.

Reportable Occurrence. An incident that shall be reported to the DOE incident reporting and process system and other federal or state agencies. The threshold for reporting will be provided in the RPP-WTP incident reporting procedure to be developed in Part B.

Requirements. Standards that are mandated by an authority through statute, regulations, and contract.

Restricted Area (DOE/RL-96-0006 [DOE-RL 1996b]). An area identified by the Contractor to which access is limited for the purposes of protecting individuals against undue risk from exposure to radiation and radioactive materials. Only a radiation worker is allowed into this area.

Risk (AIChE 1992). The combination of the expected frequency (events/year) and consequence (effects/event) of a single accident or a group of accidents.

Risk Assessment (AIChE 1992). The systematic application of management policies, procedures, and practices to the tasks of analyzing and controlling risk in order to protect employees, the general public, the environment, and company assets.

Safe State (DOE/RL-96-0006 [DOE-RL 1996b]). A situation in which the facility process has been rendered safe and no pressurized material flow occurs in the process lines. Any active, energy generating, process reactions are in controlled or passive equipment. The structures, systems, and components necessary to reach and maintain this condition are functioning in a stable manner, with all process parameters within normal safe state ranges.

Safety Analysis Report (DOE/RL-96-0006 [DOE-RL 1996b]). A document that fully describes the analyzed safety basis for the facility (safety envelope), fully demonstrates that the facility will perform and will be operated such that radiological, nuclear, and process safety requirements are met, and fully demonstrates adequate protection of the public, the workers, and the environment.

Safety Criterion. A measurable and/or demonstrable statement of an expected condition that ensures adequate protection of the public and workers. In satisfying the full set of Safety Criteria, the Project ensures that an acceptable status or condition protecting the public and/or workers has been achieved and/or maintained.

Safety Design Class. Structures, systems, or components that, by performing their specified safety function, prevent workers or the maximally exposed member of the public from receiving a radiological or chemical exposure that exceeds the accident exposure standards defined in the SRD. Those features credited for the prevention of a criticality event are also designated as Safety Design Class.

Safety Design Significant. Structures, systems, and components needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that can, if they fail or malfunction, place frequent demands on, or adversely affect the function of, Safety Design Class SSCs.

Safety Limits (DOE/RL-96-0006 [DOE-RL 1996b]). Limits on process variables associated with those physical barriers, generally passive, that are necessary for the intended facility safety functions and that are found to be required to prevent release of unacceptable levels of radioactive material to workers or the general public.

Specified Safety Function. That attribute of a Safety Design Class or Safety Design Significant engineered control credited for maintaining public or worker safety within exposure standards.

Safety Requirements Document (SRD)(DOE/RL-96-0006 [DOE-RL 1996b]). A document that contains the approved and mandated set of radiological, nuclear, and process safety standards and requirements which, if implemented, provides adequate protection of workers, the public, and the environment against the hazards associated with the operation of the Contractor's facilities.

Start of Cold-Testing. That point in the construction phase of each facility of the RPP-WTP during start-up testing but prior to admitting any significant quantities of radioactive waste or process chemicals into the facility. This milestone will be established in the Construction Agreement.

Tailoring (DOE G 450.4-1). Adapting something, such as a safety program, practice, or requirement to suit the need or purposes of a particular operation or activity, taking into account the type of work and associated hazards and hazardous situations.

Technical Safety Requirements (DOE/RL-96-0006 [DOE-RL 1996b]). Those requirements that define the conditions, the safe boundaries, and the management or administrative controls necessary to ensure the safe operation of the facility, reduce the potential risk to the public and facility workers from uncontrolled releases of radioactive materials, and from radiation exposures due to inadvertent criticality.

Unreviewed Safety Question (USQ) (DOE/RL-96-0006 [DOE-RL 1996b]). A safety question where any of the following conditions are satisfied: 1) the probability of occurrence or the radiological consequences of an accident or malfunction of equipment important to safety, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility analysis, may be increased; 2) a possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis may be created; or 3) any margin of safety is reduced. (Also see definition for "Margin of Safety".)

Validation. As applied to procedures, validation is the process that ensures an administrative control provides sufficient and understandable guidance and direction to the craft person and that it is compatible with the equipment or system being maintained. Validation is typically performed in the field prior to initial procedure use.

Verification. As applied to procedures, verification is the review to ensure the proper format and technical accuracy of a new or revised procedure. This review also ensures that the format incorporates human factors principles and other appropriate administrative policies.

Worker (DOE/RL-96-0006 [DOE-RL 1996b]). Worker means an individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities.

13.0 References

62 FR 8693, "Record of Decision for the Tank Waste Remediation System, Hanford Site, Richland, Washington", U.S. Department of Energy, *Federal Register*, Vol. 62, pp. 8693-8704.

10 CFR 20, "Standards for Protection Against Radiation", *Code of Federal Regulations*, as amended.

10 CFR 820, "Procedural Rules for DOE Nuclear Activities", *Code of Federal Regulations*, as amended.

10 CFR 830.120, "Quality Assurance Requirements", *Code of Federal Regulations*, as amended.

10 CFR 835, "Occupational Radiation Protection", *Code of Federal Regulations*, as amended.

10 CFR 1021.216, "Procurement, Financial Assistance, and Joint Ventures", *Code of Federal Regulations*, as amended.

29 CFR 1910, "Occupational Safety and Health Standards", *Code of Federal Regulations*, as amended.

40 CFR 68, "Chemical Accident Prevention Provisions", *Code of Federal Regulations*, as amended.

AIChE 1992, *Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York.

AIHA 1988, *Emergency Response Planning Guidelines*, American Industrial Hygiene Association, Akron, Ohio.

ASME 1989, *Quality Assurance Requirements for Nuclear Facility Applications*, ASME NQA-1-1989 Edition, American Society of Mechanical Engineers, Fairfield, New Jersey.

BNFL 1997a, *Quality Assurance Program*, BNFL-5193-QAP-01, BNFL Inc., Richland Washington.

BNFL 1997b*, Hazard Analysis Report,* BNFL-5193-HAR-01, BNFL Inc., Richland, Washington

BNFL 1997c, *Initial Safety Analysis Report*, BNFL-5193-ISA-01, BNFL Inc, Richland, Washington.

BNFL 1997d, *Safety Requirements Document*, BNFL-5193-SRD-01, BNFL Inc., Richland, Washington. (Revision 2 issued December 1998).

BNFL 1997e, *Radiological and Nuclear Dose Standards for Facility and Co-Located Worker*, BNFL Inc., Richland, Washington.

BNFL 1998a, *Deactivation Plan*, BNFL-5193-DP-01, Draft, BNFL Inc., Richland, Washington.

BNFL 1998b, *Integrated Master Plan*, BNFL-5193-IMP-01, Revision 1, BNFL Inc., Richland, Washington.

BNFL 1998c, *Quality Assurance Program and Implementation Plan*, BNFL-5193-QAP-01, BNFL Inc., Richland, Washington.

BNI 2001, *Quality Assurance Manual*, 24590-WTP-QAM-QA-01-001, Bechtel National, Inc., Richland, Washington.

BNI 2001a, *Quality Assurance Provisions Document*, 24590-WTP-QPD-QA-01-001, Bechtel National, Inc., Richland, Washington.

BNI 2001b, *Safety Requirements Document, Volume I*, 24590-WTP-SRD-01-001-01, Bechtel National, Inc., Richland, Washington.

BNI 2001c, *Safety Requirements Document, Volume II*, 24590-WTP-SRD-01-001-02, Bechtel National, Inc., Richland, Washington.

BNI 2001d, *Initial Safety Analysis Report, Volume I*, 24590-WTP-ISAR-01-001-01, Bechtel National, Inc., Richland, Washington.

BNI 2001e, *Initial Safety Analysis Report, Volume II*, 24590-WTP-ISAR-01-001-02, Bechtel National, Inc., Richland, Washington.

BNI 2001f, *RPP-WTP Configuration Management Plan*, 24590-WTP-PL-MG-01-002, Bechtel National, Inc., Richland, Washington.

DOE 1994, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*, DOE-HDBK-3010-94, U.S. Department of Energy, Washington, D.C.

DOE 1995a, *Comprehensive Emergency Management System*, DOE O 151.1, U.S. Department of Energy, Washington, D.C.

DOE 1999, *Quality Assurance*, DOE Order 414.1A, September 29, 1999, US Department of Energy, Washington, DC.

DOE 1999a, *Contractors Requirements Document*, Attachment 1 to DOE Order 414.1A, *Quality Assurance*, September 29, 1999, US Department of Energy, Washington, DC.

DOE 2000, *Quality Assurance Requirements and Description for the Civilian Radioactive Waste Management Program (QARD)*, DOE/RW-0333P, Rev 10, April 28, 2000, U.S. Department of Energy, Washington, D.C.

DOE-ORP 2000, DOE Contract DE-AC27-01RV14136, U.S. Department of Energy, Office of River Protection, Richland, Washington.

DOE-RL 1994, *Hanford Emergency Response Plan*, DOE/RL 94-02, U.S. Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL 1996a, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0003, Revision 0, U.S. Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL 1996b, *Top-level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 0, U.S. Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL 1996c, *TWRS Privatization*, DOE Contract DE-AC06-RL-12208, U.S. Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL 1997, *Guidance for the Review of TWRS Privatization Contractor Integrated Safety Management Plan Submittal Package*, Revision 0, RL/REG-97-07, U.S. Department of Energy, Richland, Washington.

DOE-RL 1998a, *Corrective Action/Enforcement Action Program Description*, Revision 0, RL/REG-98-06, US Department of Energy, Richland, Washington.

DOE-RL 1998b, *Inspection Program Description for the Regulatory Oversight of TWRS Privatization Contractors*, Revision 0, RL/REG-98-05, US Department of Energy, Richland, Washington.

DOE-RL 2000, *Regulatory Unit Position on Contractor-Initiated Changes to the Authorization Basis*, Revision 7, RL/REG-97-13, US Department of Energy, Office of Safety Regulation of the Contractor, Richland, Washington.

DOE-RL 2001, *Review Guidance for the Construction Authorization Request (CAR)*, Revision 3, RL/REG-99-05, US Department of Energy, Richland, Washington.

EPA 1991, *Manual of Protective Action Guides and Protective Actions for Nuclear Incidents*, US Environmental Protection Agency, Washington, D.C.

Gibbs, D C, 2000, "Approval of BNFL-5193-QAP-01, Rev 4c, 'Quality Assurance Program and Implementation Plan' (QAPIP)", 00-RU-0063, (letter to Mr. M J Bullock, BNFL Inc., January 7, 2000), U S Department of Energy, Richland Operations Office, Richland, Washington.

HRC 1976, *Investigation of Incident in Ion Exchange Resin*, HRC Report 3719, Hazards Research Corporation, Denville, New Jersey.

ICBO 1994, *Uniform Building Code*, International Conference of Building Officials, Whittier, California.

National Environmental Policy Act, 42 USC 4321 et seq., as amended.

NCRP 1963, *Maximum Permissible Body Burdens and Maximum Permissible Concentrations of Radionuclides in Air and in Water for Occupational Exposure*, Handbook 69, Addendum 1, Recommendations of the National Committee on Radiation Protection, National Bureau of Standards, Washington, D.C.

NRC 1977, *Operating Philosophy for Maintaining Occupational Radiation Exposures As Low As Is Reasonably Achievable*, Regulatory Guide 8.10, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1978, *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations is be As Low as is Reasonably Achievable*, Regulatory Guide 8.8, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1982, *Accident Generated Particulate Materials and Their Characteristics -- A Review of Background Information*, NUREG/CR-2651, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1988, *Nuclear Fuel Cycle Accident Analysis Handbook*, NUREG-1320, in revision, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1994, *Integrated Safety Analysis Guidance Document*, NUREG-1513, draft, distributed August 8, 1994, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1995a, *Standard Format and Content for the Health and Safety Sections of License Applications for Fuel Cycle Facilities*, Regulatory Guide 3.52, Revision 2, draft, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1995b, *Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility*, draft NUREG-1520, U.S. Nuclear Regulatory Commission, Washington, D.C.

Resource Conservation and Recovery Act of 1976, 42 USC 2795 et seq., as amended.

Sheridan, T. R., 1997, "TWRS Regulatory Unit Approval of the BNFL, Inc. 'Tank Waste Remediation System Privatization Project Quality Assurance Program'", BNFL-5193-QAP-01, Revision 2, February 7, 1997", 97-RU-0042, (letter to Mr. Maurice J. Bullock, BNFL, February 12), U.S. Department of Energy, Richland Operations Office, Richland, Washington.

State Environmental Policy Act, Chapter 43.21C, Revised Code of Washington.

WAC 173-303, "Dangerous Waste Regulations", *Washington Administrative Code*, as amended.

WAC 173-400, "Washington State Air Pollution Control Regulations", *Washington Administrative Code*, as amended.

WAC 173-460, "Controls for New Sources of Toxic Air Pollutants", *Washington Administrative Code*, as amended.

Document title:	**Safety Requirements Document Volume II**
Contract number:	DE-AC27-01RV14136
Department:	Environmental, Safety, and Health
Document number:	24590-WTP-SRD-ESH-01-001-02, Rev 0c
Date of issue:	20 February 2002
Issue status:	Approved

History Sheet

Rev	Date	Reason for revision	Revised by
0	21 Sep 2001	Supersedes BNFL-5193-SRD-01-02 Rev 5. Incorporates 24590-WTP-ABCN-ESH-01-017 Rev 0 changes (contractor-approved ABCN).	K Gibson
0a	4 Oct 2001	Incorporates ABCN-24590-01-00006 Rev 0 changes as partially approved by DOE Letter 01-OSR-0311 (CCN 023253) and contractor approved as revised ABCN-24590-01-00006, Rev 1.	K Gibson
0b	19 Feb 2002	Incorporates ABCN-24590-01-00004 Rev 2 changes as approved (with editorial changes specified) by DOE Letter 02-OSR-0034 (CCN 028170).	K Gibson
0c	20 Feb 2002	Incorporates 24590-WTP-ABCN-ESH-01-013 Rev 1 as approved by DOE Letter 02-OSR-0019 (CCN 028213).	K Gibson

Revision Status

Page No.	Rev.	Page No.	Rev.	Page No.	Rev.	Page No.	Rev.
i	0c	4-15	0	7-4	0	9-11	0a
ii	0c	4-16	0a	7-5	0	9-12	0a
iii	0c	4-17	0	7-6	0a	9-13	0a
iv	0c	4-18	0	7-7	0a	9-14	0a
v	0a	4-19	0	7-8	0a	A-i	0
vi	0b	4-20	0	7-9	0	A-ii	0
1-1	0a	4-21	0	7-10	0	A-1	0
1-2	0	4-22	0	7-11	0a	A-2	0
1-3	0a	4-23	0	7-12	0a	A-3	0
1-4	0	4-24	0	7-13	0	A-4	0
2-1	0	4-25	0	7-14	0a	A-5	0a
2-2	0	4-26	0	7-15	0	A-6	0
2-3	0a	4-27	0	7-16	0	A-7	0
3-1	0a	4-28	0	7-17	0a	A-8	0
3-2	0a	4-29	0	7-18	0	A-9	0
3-3	0a	4-30	0	7-19	0a	A-10	0
3-4	0a	4-31	0	7-20	0a	A-11	0a
3-5	0a	4-32	0a	7-21	0a	A-12	0
3-6	0	5-1	0	7-22	0	A-13	0
3-7	0	5-2	0	7-23	0	A-14	0
3-8	0	5-3	0	7-24	0	A-15	0
3-9	0	5-4	0	7-25	0a	A-16	0
4-1	0a	5-5	0	7-26	0a	A-17	0
4-2	0	5-6	0	7-27	0a	A-18	0
4-3	0	5-7	0	8-1	0	A-19	0
4-4	0c	5-8	0	9-1	0	A-20	0
4-5	0c	5-9	0	9-2	0	B-i	0
4-6	0	5-10	0	9-3A	0b	B-ii	0
4-7	0	5-11	0	9-3B	0b	B-1	0
4-8	0c	5-12	0	9-4	0b	B-2	0
4-9	0c	5-13	0	9-5	0a	B-3	0
4-10	0c	6-1	0a	9-6	0	B-4	0
4-11	0	6-2	0a	9-7	0	B-5	0
4-12	0	7-1	0	9-8	0	B-6	0
4-13	0	7-2	0	9-9	0	B-7	0
4-14	0	7-3	0a	9-10	0a	B-8	0

Page No.	Rev.	Page No.	Rev.	Page No.	Rev.	Page No.	Rev.
B-9	0	C-4	0	D-4	0	G-5	0b
B-10	0	C-5	0	D-5	0	G-6	0b
B-11	0	C-6	0	D-6	0	G-7	0b
B-12	0	C-7	0	D-7	0	G-8	0b
B-13	0	C-8	0	D-8	0	G-9	0b
B-14	0	C-9	0	D-9	0	G-10	0b
B-15	0	C-10	0	D-10	0	G-11	0b
B-16	0	C-11	0	D-11	0	G-12	0b
B-17	0	C-12	0c	D-12	0	G-13	0b
B-18	0	C-13	0	E-i	0	G-14	0b
B-19	0	C-14	0	E-1	0	G-15	0b
B-20	0	C-15	0	E-2	0	G-16	0b
B-21	0	C-16	0	F-i	0	G-17	0b
B-22	0	C-17	0c	F-ii	0	G-18	0b
B-23	0	C-18	0c	F-1	0	G-19	0b
B-24	0	C-19	0c	F-2	0	G-20	0b
B-25	0	C-20	0c	G-i	0b	G-21	0b
C-i	0	D-i	0	G-ii	0b	G-22	0b
C-ii	0	D-ii	0	G-1	0b	G-23	0b
C-1	0	D-1	0	G-2	0b	G-24	0b
C-2	0	D-2	0	G-3	0b	G-25	0b
C-3	0	D-3	0	G-4	0b		

* These pages added at this revision; therefore, no revision bars are used to indicate changes.

Approved by: _____ _____ Date: _____
(Print name) (Sign)

CONTENTS

1.0 Radiological, Nuclear and Process Safety Objectives....1-1
2.0 Radiological and Process Standards....2-1
3.0 Nuclear and Process Safety....3-1
3.1 Hazards Analysis....3-1
3.2 Accident Analysis....3-6
3.3 Criticality....3-7
4.0 Engineering and Design....4-1
4.1 General Design....4-3
4.2 Confinement Design....4-11
4.3 Engineered Safety Systems....4-13
4.4 Electrical and Mechanical Systems....4-17
4.5 Fire Protection....4-26
5.0 Radiation Protection....5-1
5.1 Occupational Radiation Protection....5-1
5.2 Occupational Radiation Protection Design....5-6
5.3 Environmental Radiation Protection....5-7
5.4 Environmental Radiological Monitoring....5-12
6.0 Startup....6-1
7.0 Management and Operations....7-1
7.1 Management and Organization/Staffing....7-3
7.2 Training and Procedures....7-5
7.3 Quality Assurance Program....7-9
7.4 Unreviewed Safety Questions....7-14
7.5 Conduct of Operations....7-16
7.6 Maintenance....7-17
7.7 Reporting and Incident Investigation....7-20
7.8 Emergency Preparedness....7-25
8.0 Deactivation and Decommissioning....8-1
9.0 Documentation and Submittals....9-1
9.1 Safety Analysis Reports....9-3
9.2 Technical Safety Requirements....9-6
9.3 Risk Management Plan (this section has been deleted)....9-10

APPENDICES

Appendix A Implementing Standard for Safety Standards and Requirements Identification.....A-i
Appendix B Implementing Standard for Defense in Depth .....B-i
Appendix C Implementing Standards .....C-i
Appendix D Radiological Exposure Standards for the RPP-WTP Project .....D-i
Appendix E Reliability, Availability, Maintainability, and Inspectability (RAMI).....E-i
Appendix F Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning..... F-i
Appendix G Ad Hoc Implementing Standard for Safety Analysis Reports.....G-i

1.0 Radiological, Nuclear and Process Safety Objectives

Safety Criterion: 1.0 - 1

A comprehensive radiological and process safety management program shall be used to eliminate or reduce the incidence, or mitigate the consequences of, accidental radioactive or chemical releases, process fires, and process explosions. This program shall address management practices, technologies, and procedures. Radiological and process safety management shall confirm that the facility is properly designed, the integrity of the design is maintained, and the facility is operated according to the safe manner intended.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 4.1 Safety Management Processes
Chapter: 5.0 Process Safety Management

Regulatory Basis

DOE/RL-96-0006 5.1.1 Process Safety Management
DOE/RL-96-0006 5.1.2 Process Safety Objective

Safety Criterion: 1.0 - 2

Principal emphasis shall be placed on the prevention of accidents, particularly any that could cause an unacceptable release, as the primary means of achieving safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2

Regulatory Basis

DOE/RL-96-0006 4.1.1.2 Defense in Depth-Prevention

Safety Criterion: 1.0 - 3

The risk, to an average individual within 1 mile of the RPP-WTP Controlled Area Boundary, of prompt fatalities that might result from an accident shall not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents which members of the U.S. population generally are exposed.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 3.1.2 Accident Risk Goal

Safety Criterion: 1.0 - 4

The risk, to the public and workers within 16 km (10 miles) of the RPP-WTP, of cancer fatalities that might result from RPP-WTP operations shall not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks to which members of the U.S. population generally are exposed.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

test change

Regulatory Basis

DOE/RL-96-0006 3.1.1 Operations Risk Goal

Safety Criterion: 1.0 - 5

The risk to workers within the RPP-WTP Controlled Area Boundary, of fatality from radiological exposure that might result from an accident, shall not be a significant contributor to the overall occupational risk of fatality to workers.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 3.1.3 Worker Accident Risk Goal

Safety Criterion: 1.0 - 6

Measures in the design and operation of the facility to protect the public, workers, and environment against accident conditions shall be evaluated using an acceptable approach to demonstrate that they perform their intended purpose with high confidence.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 3.3.1 Public Protection

DOE/RL-96-0006 3.3.2 Worker Protection

Safety Criterion: 1.0 - 7

To compensate for potential human and equipment failures, a defense-in-depth strategy shall be applied to the facility commensurate with the hazards; such that, as appropriate to control the risk, safety is vested in multiple, independent safety provisions, no one of which is to be relied upon excessively to protect the public, the workers, or the environment. This strategy shall be applied to the design and operation of the facility.

Implementing Codes and Standards

ANSI/ANS 58.9-1981 Single Failure Criteria for Light Waster Reactor Safety-Related Fluid Systems
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety 4.1.1.2
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006 *4.1.1.1 Defense in Depth-Defense in Depth*

Safety Criterion: 1.0 - 8

Structures, systems, and components (SSCs) that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public are classified as Important to Safety. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation). This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of Important to Safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Important to Safety includes SSCs designated as Safety Design Class and Safety Design Significant.

Safety Design Class SSCs includes those that, by performing their specified safety function, prevent workers or the maximally exposed member of the public from receiving a radiological or chemical exposure that exceeds the exposure standards defined in the SRD. Those features credited for the prevention of a criticality event are also designated as Safety Design Class.

Safety Design Significant SSCs are those needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that can, if they fail or malfunction, place frequent demands on, or adversely affect the function of, Safety Design Class SSCs.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006	*3.3.1*	*Public Protection*
DOE/RL-96-0006	*3.3.2*	*Worker Protection*

Safety Criterion: 1.0 - 9

The RPP-WTP Contractor shall accept responsibility for the safety of the RPP-WTP.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 1.0 Project Safety Approach
Section: 11.1 Design and Construction Phase
Section: 11.2 Operations Phase

Regulatory Basis

DOE/RL-96-0006	*4.1.2.1*	*Safety Responsibility-Safety Responsibility*
DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*
DOE/RL-96-0006	*5.1.3*	*Process Safety Responsibility*

Safety Criterion: 1.0 - 10

In addition to the Safety Criteria contained herein, compliance with all requirements of 10 CFR 830.120 and 10 CFR 835 shall be achieved absent the granting of an exemption request to any specific requirement therein.

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location*
10 CFR 835	*Occupational Radiation Protection*	*Location: 1*
DE-AC06-96RL13308	*Part I Section C.5 Table S4-1*	

2.0 Radiological and Process Standards

Safety Criterion: 2.0 - 1

The following Radiological Dose Standards shall be applied to protect the public and workers from RPP-WTP radiological hazards.

Table 2-1. Radiological Exposure Standards Above Normal Background (Sheet 1)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Normal Events Events that occur regularly in the course of facility operation (e.g., normal facility operations); including routine and preventive maintenance activities.	>0.1	Normal modes of operating facility systems should provide adequate protection of health and safety.	≤5 rem/yr ≤50 rem/yr any organ, skin, or extremity ≤15 rem/yr lens of eye ≤1.0 rem/yr ALARA design objective per 10CFR835.1002(b)(1)	≤5 rem/yr ≤1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b)(1)	≤10 mrem/yr (airborne pathway) ≤100 mrem/yr (all sources) ≤100 mrem/yr (public in the controlled area) ≤25 mrem/yr (radioactive waste)
Anticipated Events Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	$10^{-2}<f\leq10^{-1}$	The facility should be capable of returning to operation without extensive corrective action or repair.	≤5 rem/event (2,3) 1.0 rem/event design action threshold (4)	≤5 rem/event (2, 3) 1.0 rem/event design action threshold(4)	≤100 mrem/event(3)
Unlikely Events Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	$10^{-4}<f\leq10^{-2}$	The facility should be capable of returning to operation following potentially extensive corrective action or repair, as necessary.	≤25 rem/event(2,3)	≤25 rem/event(2, 3)	≤5 rem/event(3)

Table 2-1. Radiological Exposure Standards Above Normal Background (Sheet 2)

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Extremely Unlikely Events Events that are not expected to occur during the life of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.	$10^{-6}<f\leq10^{-4}$	Facility damage may preclude returning to operation.	≤25 rem/event(2,3)	≤25 rem/event(2,3)	≤25 rem/event ≤5 rem/event target(3) ≤300 rem/event to thyroid
Location of Receptor			Within the RPP-WTP Controlled Area Boundary	The most limiting location at or beyond the RPP-WTP Controlled Area Boundary	The most limiting location along the near river bank/ Hwy240/ southern boundary

Notes
(1) In addition to meeting the listed design objective of 10 CFR 835.1002(b), the inhalation of radioactive material by workers and collocated workers under normal conditions is kept ALARA through the control of airborne radioactivity as described in 10 CFR 835.1002(c).

(2) In addition to meeting the listed worker and collocated worker exposure standards for accidents, the Worker Accident Risk Goal is satisfied through the calculation of the risk from accidents with accident prevention and mitigation features added as necessary to meet the Goal.

(3) In addition to meeting the listed exposure standards for accidents, the approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below standards to account for uncertainties in the analysis, and to provide for sufficient design margin and operational flexibility.

(4) When a calculated accident exposure exceeds this threshold, then appropriate actions are taken. These include carrying out a less bounding (i.e., more realistic) evaluation to show that the accident consequences will be below the threshold or evaluating additional safeguards for cost-effectiveness and/or feasibility. This threshold is not a limit; it does not require the implementation of additional preventative or mitigative features if they are not both cost-effective and feasible.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006 2.1 Individual (Dose Standards Above Normal Background)

Safety Criterion: 2.0 - 2

The following dose standards shall be applied to protect the public and workers from RPP-WTP chemical hazards.

Releases exposing the offsite public to ERPG-2 concentrations (AIHA 1999)

Releases exposing the co-located worker to ERPG-3 concentrations (AIHA 1999)

Accidents affecting the facility worker that could cause in-patient hospitalization of at least 3 facility workers, or at least a single fatality.

Where ERPG values have not been published, the DOE Temporary Emergency Exposure Limits (TEELs) may be used as substitute ERPGs.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 2.0 - 3

In addition to the dose limits specified for the public in Safety Criterion 2.0-1 Table 2-1, the dose in any unrestricted area from external sources shall not exceed 0.002 rem in any one hour.

Implementing Codes and Standards

DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

WAC 246-221 Radiation Protection Standards Location: 060 (1)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 040 (2)

3.0 Nuclear and Process Safety

3.1 Hazards Analysis

Safety Criterion: 3.1 - 1

An initial process hazard analysis (hazard evaluation) shall be performed using acceptable industry practices. The analysis shall include consideration of both chemical and radiological hazards. The process hazard analysis shall be appropriate to the complexity of the process and shall identify, evaluate, and document the design features which control the hazards involved in the process.

The process hazard analysis shall be performed by a team with expertise in engineering and process operations, and the team shall include at least one member who has experience and knowledge specific to the process being evaluated. Also, one member of the team must be knowledgeable in the specific process hazard analysis methodology being used.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 2

A compilation of written process safety information appropriate to the stage of design being considered shall be completed to support the process hazard analysis. The compilation of written process safety information enables the employer and the employees involved in operating the process to identify and understand the hazards posed by those processes involving radioactive materials and process chemicals considered to pose a hazard. This process safety information shall include information pertaining to the hazards of the materials used or produced by the process, information pertaining to the technology of the process, and information pertaining to the equipment in the process.

(1) Information pertaining to the hazards of the materials in the process including:
   - (a) Toxicity information
   - (b) Permissible exposure limits
   - (c) Physical data
   - (d) Reactivity data
   - (e) Corrosivity data
   - (f) Thermal and chemical stability data
   - (g) Hazardous effects of inadvertent mixing of different materials that could foreseeably occur

(2) Information pertaining to the technology of the process including at least the following:
   (a) A block flow diagram or simplified process flow diagram
   (b) Process chemistry
   (c) Maximum intended inventory
   (d) Safe upper and lower limits for such items as temperatures, pressures, flows or compositions
   (e) An evaluation of the consequences of deviations, including those affecting the safety and health of employees

(3) Information pertaining to the equipment in the process including:
   (a) Materials of construction
   (b) Process drawings or piping and instrument diagrams (P&IDs)
   (c) Electrical classification
   (d) Relief system design and design basis
   (e) Ventilation system design
   (f) Design codes and standards employed
   (g) Material and energy balances
   (h) Safety systems (e.g. interlocks, detection or suppression systems)

The records shall be maintained documenting that equipment complies with recognized and generally accepted good engineering practices. The safety information shall be kept up-to-date.

Implementing Codes and Standards

Regulatory Basis

DOE/RL-96-0006	*5.2.1*	*Process Safety Information*
DOE/RL-96-0006	*5.2.2*	*Process Hazard Analysis*

Safety Criterion: 3.1 - 3

The process hazard analysis shall address:

(1) The hazards of the process

(2) Engineering and administrative controls applicable to the hazards and their interrelationships such as appropriate application of detection methodologies to provide early warning of releases. (Acceptable detection methods might include process monitoring and control instrumentation with alarms, and detection hardware.)

(3) Consequences of failure of engineering and administrative controls

(4) Facility siting

(5) Human factors

(6) A qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace

(7) Common-mode and common-cause failure events

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 4

The hazard analysis shall be performed in accordance with the following requirements:

(1) The consequences of unmitigated releases of radioactive material and process chemicals considered to pose a hazard shall be evaluated.

(2) The hazard analysis shall be based on an inventory of all radioactive and hazardous nonradioactive materials that are stored, utilized, or may be formed within the facility.

(3) The hazard analysis shall identify energy sources or processes that might contribute to the generation or uncontrolled release of radioactive or process chemicals considered to pose a hazard. The hazard analysis shall estimate the consequences of accidents in which the facility or process and/or materials in the inventory are assumed to interact, react, or be released in a manner to produce a threat or challenge to the health and safety of individuals on-site and off site.

(4) The risks that hazardous inventories and energy sources present shall be evaluated by consideration of normal operation (including startup, testing, and maintenance), anticipated operational occurrences, and accident conditions. The identification of anticipated operational occurrences and accident conditions shall consider internal events (i.e., equipment failure and human error), external events (e.g., nearby facilities and transportation), and natural phenomena.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006	*3.3.3*	*Accident Vulnerability Mitigation*
DOE/RL-96-0006	*5.2.2*	*Process Hazard Analysis*

Safety Criterion: 3.1 - 5

A written plan of action shall be developed regarding employee participation in the conduct and development of process hazards analyses and on the development of process safety management. Employees and their representatives shall be consulted on the conduct and development of process hazards analyses and on the development of the other elements of process safety management. Employees and their representatives shall be provided access to process hazard analyses and other information developed related to process safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

Safety Criterion: 3.1 - 6

A system shall be established to promptly address the hazard analysis team's findings and recommendations; assure that the recommendations are resolved in a timely manner; and that the resolution is documented. The contractor shall document what actions are to be taken; complete actions; develop a written schedule of when these actions are to be completed; communicate the actions to operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02
Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 7

The process hazard analysis shall be updated to reflect changes concurrently with the annual update of the FSAR by a qualified team, to assure that the process hazard analysis is consistent with the current process.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation
Section: 5.6.2 Updating of the Hazard Analysis Report

Regulatory Basis

DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 8

Employers shall retain process hazards analyses and updates or revalidations as well as the documented resolution of any recommendations for the life of the process.

Implementing Codes and Standards

Regulatory Basis

3.2 Accident Analysis

Safety Criterion: 3.2 - 1

Acceptable risk analyses shall be applied during the design to delineate provisions for the prevention and mitigation, including emergency preparedness and response, of otherwise risk-dominant events.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3 Description of the Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 4.2.1.2 Design-Risk Assessment

3.3 Criticality

Safety Criterion: 3.3 - 1

The facility shall be designed and operated in a manner that prevents nuclear criticality.

Implementing Codes and Standards

ANSI/ANS 8.1-1983 (R 1988) Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors

ANSI/ANS 8.19-1996 Administrative Practices for Nuclear Criticality Safety

Regulatory Basis

DOE/RL-96-0006 4.2.2.5 Proven Engineering Practices/Margins-Criticality

Safety Criterion: 3.3 - 2

The design of handling, packaging, transfer, and storage systems must include margins of safety for the nuclear criticality parameters that are commensurate with the uncertainties in the data and methods used in calculations and in the nature of the immediate environment under accident conditions.

The multiplication factor (k<eff>), including all biases and uncertainties at a 95% confidence level, shall be shown to not exceed 0.95 under all credible normal, off-normal, and accident conditions.

Safety Criterion: 3.3 - 3

Process designs shall incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible. Protection shall be provided by either:

(1) the control of two independent process parameters (which is the preferred approach, when practical, to prevent common-mode failure), or

(2) a system of multiple controls on a single process parameter.

The number of controls required for a single controlled process parameter shall be based upon control reliability and any features that mitigate the consequences of control failure. In all cases, no single credible event or failure shall result in the potential for a criticality accident.

An exception to the application of double contingency, where single contingency operations are permissible, is presented in paragraph 5.1 of ANSI/ANS-8.10-1983, R88. This exception applies to operations with shielding and confinement (e.g., hot cells or other shielded facilities).

Double contingency shall be demonstrated by documented evaluations.

Safety Criterion: 3.3 - 4

Where a sufficient quantity of fissionable material is being processed such that criticality safety is a concern, passive engineered controls, such as geometry control, shall be considered as the preferred control method. Where passive engineered control is not feasible, the preferred order of controls is active engineered controls followed by administrative controls. The double contingency analysis shall justify the chosen controls. Full advantage may be taken of any nuclear characteristics of the process materials and equipment. The geometry must be considered as water moderated and reflected unless it can be shown the presence of water is not credible. All dimensions, nuclear properties, and other features upon which reliance is placed shall be documented and verified prior to beginning operations, and control shall be exercised to maintain them.

Safety Criterion: 3.3 - 5

To protect against an uncontrolled nuclear criticality incident, nuclear criticality safety considerations and controls shall be evaluated for accidents, normal operations, and before any significant operational changes are made.

Safety Criterion: 3.3 - 6

Criticality Accident Alarm Systems (CAS) and Criticality Detection Systems (CDS) shall be required as follows:

(1) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material and the probability of a criticality accident is greater than 1E-06 per year, a CAS conforming to ANSI/ANS-8.3-1986 shall be provided to cover occupied areas in which the expected dose exceeds 12 rads (0.12 greys) in free air, where a CAS is defined to include a criticality accident detection device and a personnel evacuation alarm.

(2) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material and the probability of a criticality accident is greater than 1E-06 per year, but there are no occupied areas in which the expected dose exceeds 12 rads (0.12 greys) in free air, a CDS shall be provided, where a CDS is defined to be an appropriate criticality accident detection device but without an immediate evacuation alarm. The CDS response time should be sufficient to allow for appropriate process-related mitigation and recovery actions. Appropriate response guidance to minimize personnel exposure shall be provided.

(3) In those locations where the mass of fissionable material exceeds the limits established in Table 3-1 Inventory of Fissionable Material, but a criticality accident is determined to be impossible due to the physical form of the fissionable material, or the probability of occurrence is determined to be less than 1E-06 per year, neither a CAS nor a CDS is required. Neither a CAS nor a CDS is required for fissionable material during shipment when packaged in approved shipping containers, or when packaged in approved shipping containers awaiting transport provided that no other operation involving fissionable material not so packaged is permitted on the shipping dock or in the shipment area.

(4) If a criticality accident is possible wherein a slow (i.e., quasistatic) increase in reactivity could occur leading from subcriticality to criticality to self-shutdown without initiating emplaced criticality alarms, CASs should be supplemented by warning devices such as audible personnel dosimeters (e.g., pocket chirpers/flashers, or their equivalents), area radiation monitors, area dosimeters, or integrating CASs to aid in protecting workers against the consequences of slow criticality accidents.

(5) Neither a CAS nor a CDS is required to be installed for handling or storage of fissionable material when sufficient shielding exists that is adequate to protect personnel (e.g., hot cells); however, a means to detect fission product gases or other volatile fission products shall be provided in occupied areas immediately adjacent to such shielded areas, except for systems where no fission products are likely to be released.

Note: The frequency of 1E-06 per year is used as a measure of credibility and does not require a probabilistic risk assessment be performed. Reasonable grounds for incredibility may be presented on the basis of commonly accepted engineering judgement.

Table 3-1. Inventory of Fissionable Material[1]

Isotope	Inventory in Individual Unrelated Area
U-235	700g
U-233	520g
Pu-239	450g
Any Combination of above Isotopes	450g

[1] Per ANSI/ANS-8.3-1986 paragraph 4.2.1

Safety Criterion: 3.3 - 7

The monitoring system shall be capable of detecting a criticality that produces an absorbed dose in soft tissue of 20 rads (0.20 greys) of combined neutron and gamma radiation at an unshielded distance of 2 meters from the reacting material within one minute.

Safety Criterion: 3.3 - 8

Coverage of all areas requiring detection may be provided by a single detector.

4.0 Engineering and Design

Safety Criterion: 4.0 - 1

Formal configuration management shall be applied to all facility activities through deactivation of the RPP-WTP to ensure that programmatic objectives, including safety, are fully achieved. Work shall be performed and controlled according to pre-approved plans and procedures that clearly delineate responsibility. Documented records shall be retained.

Implementing Codes and Standards
ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis
DOE/RL-96-0006 4.1.5.1 Configuration Management-Formal Configuration Management

Safety Criterion: 4.0 - 2

Written procedures shall be established and implemented to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures; and, changes to facilities that affect a covered process. The procedures shall assure that the following considerations are addressed prior to any change:

(1) The technical basis for the proposed change

(2) Impact of change on safety and health

(3) Modifications to operating procedures

(4) Necessary time period for the change

(5) Authorization requirements for the proposed change

Employees involved in operating a process and maintenance and subcontract employees whose job tasks will be affected by a change in the process shall be informed of, and trained in, the change prior to start-up of the process or affected part of the process. If a change covered by this paragraph results in a change in the process safety information, such information shall be updated accordingly. If a change covered by this paragraph results in a change in operating procedures or practices, such procedures or practices shall be updated accordingly.

Implementing Codes and Standards
ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis
DOE/RL-96-0006 5.2.9 Management of Change

Safety Criterion: 4.0 - 3

A system shall be used to control and maintain accurate as-built records for Important to Safety SSCs through deactivation of the facility.

Implementing Codes and Standards

ISO 10007 Quality Management - Guidelines for Configuration Management

Regulatory Basis

DOE/RL-96-0006 *4.1.5.3 Configuration Management-Design Documentation*

4.1 General Design

Safety Criterion: 4.1 - 1

The facility design shall provide for the prevention and mitigation of the risks associated with radiological and chemical material inventories and energy sources. The facility design shall include consideration of normal operation (including startup, testing and maintenance), anticipated operational occurrences, external events, and accident conditions.

Prevention shall be the preferred means of achieving safety.

Defense-in-depth shall be applied commensurate with the hazard to provide multiple physical and administrative barriers against undue radiation and chemical exposure to the public and workers.

Implementing Codes and Standards

ANSI/ANS 58.9-1981 Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety 4.1.1.2
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006	*4.1.1.1*	*Defense in Depth-Defense in Depth*
DOE/RL-96-0006	*4.1.1.2*	*Defense in Depth-Prevention*
DOE/RL-96-0006	*4.2.1.1*	*Design-Safety Design*

Safety Criterion: 4.1 - 2

Structures, systems, and components designated as Important to Safety shall be designed, fabricated, erected, constructed, tested, inspected, and maintained to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components designated as Important to Safety shall be maintained through deactivation of the facility.

Items and processes shall be designed using sound engineering/scientific principles and appropriate standards.

Design features that enhance the margin of safety through simplified, inherently safe, passive, or other highly reliable means to accomplish the specified safety function should be employed to the maximum extent practical.

Design work, including changes, shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled. The adequacy of design products shall be verified or validated by individuals or groups other than those who performed the work. Verification and validation work shall be completed before approval and implementation of the design.

Safety technologies incorporated into the facility design should have been proven by experience or testing and should be reflected in approved codes and standards. Significant new design features should be introduced only after thorough research and model or prototype testing at the component, system, or facility level, as appropriate, to achieve the necessary level of confidence that the design feature will perform as expected.

Implementing Codes and Standards

ACI 318-99, *Building Code Requirements for Structural Concrete*
ACI 318R-99, *Commentary on Building Code Requirements for Structural Concrete*
ACI 349-01, *Code Requirements for Nuclear Safety-Related Concrete Structures*
ACI 349R-01, *Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures*
AISC MO16-89, *Manual for Steel Construction - Allowable Stress Design, Ninth Edition*
ANSI/AISC N690-94, *Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities*
ASCE 4-98, *Seismic Analysis of Safety-Related Nuclear Structures and Commentary*
ASCE 7-95, *Minimum Design Loads for Buildings and Other Structures*
DOE-STD 1020-94 (Change 1, 1996), *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*
1997, *UBC Uniform Building Code*
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
ACI 530-99, *Building Code Requirements for Masonry Structures and Commentary*
24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix A, "Implementing Standard for Safety Standards and Requirements Identification"
ISO 10007, *Quality Management - Guidelines for Configuration Management*
ASTM D3740, *Standard Practice for Minimum Requirements for Agencies Engaged in the Testing and/or Inspection of Soil and Rock as Used in Engineering Design and Construction*
ASTM D2922, *Standard Test Method for Laboratory Determination of Moisture Content of Soil*
ASTM D3017, *Standard Test Method for Water Content of Soil and Rock in Place by Nuclear Methods*

Regulatory Basis

DOE/RL-96-0006	*4.1.2.4*	*Safety Responsibility-Operating Experience and Safety Research*
DOE/RL-96-0006	*4.1.5.1*	*Configuration Management-Formal Configuration Management*
DOE/RL-96-0006	*4.1.6.2*	*Quality Assurance-Established Techniques and Procedures*
DOE/RL-96-0006	*4.2.2.1*	*Proven Engineering Practices/Margins-Proven Engineering Practices*
DOE/RL-96-0006	*4.2.2.3*	*Proven Engineering Practices/Margins-Safety System Design and Qualification*
DOE/RL-96-0006	*4.2.5.1*	*Inherent/Passive Safety Characteristics-Safety Margin Enhancement*

Safety Criterion: 4.1 - 3

This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) that are Important to Safety and have NPH safety functions.

SSCs designated as Important to Safety (i.e., Safety Design Class and Safety Design Significant) shall be designed to withstand the effects of NPH events such as earthquakes, wind, and floods without loss of capability to perform specified safety functions required as the result of the NPH events. This includes both the front line and support systems that must function for a NPH event such that the public, collocated worker, or facility worker exposure standards of Safety Criterion 2.0-1 or 2.0-2 are not exceeded.

SSCs that are designated Safety Design Class (excepting those so designated based solely on chemical hazards) and that are required to perform a safety function as a result of a given NPH shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. These SSCs are designated Seismic Category I (SC-I) for earthquakes and Performance Category 3 (PC-3) for other NPH.

SSCs that are designated Safety Design Significant (excepting those so designated based solely on chemical hazards) whose continued function is not required for an NPH event, but whose failure as a result of an NPH event could reduce the functioning of a Safety Design Class SSC such that exposure standards might be exceeded, shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. For these SSCs, however, for seismic response only, credit may be taken for inelastic energy absorption per Table 2-4 of DOE-STD-1020-94. These SSCs are designated SC-II for earthquakes and PC-3 for other NPH.

For any SSC included under this criterion, other NPH loads (for which the SSC has no safety function) may be taken from Safety Criterion 4.1-4 and Table 4-2 in lieu of Safety Criterion 4.1-3 and Table 4-1.

Table 4-1 Natural Phenomena Design Loads for Important to Safety SSCs with NPH Safety Functions

Hazard	Load	Source Document for Load
Seismic	DBE with 0.26 *g* horizontal PGA and 0.18 *g* vertical PGA See Figures 4-1 and 4-2	WHC-SD-W236A-TI-002 [a] DOE-STD-1020-94[b]
Straight wind	111 mi/hr , 3-second gust, at 33 ft above ground, Importance factor, I=1.0	DOE Newsletter [c]
Wind Missile	2x4 timber plank, 15 lb at 50 mi/hr (horiz), Max height 30 ft	DOE-STD-1020-94 [b]
Tornado and Tornado Missiles	Not Applicable	DOE-STD-1020-94 [b]
Volcanic ash	12.5 lb/ft^2	HNF-SD-GN-ER-501 [d]
Flooding	Dry site for river flooding Local precipitation: 4 in. for 6 hours	HNF-SD-GN-ER-501 [d]
Snow	15.0 lb/ft^2 snow load	HNF-SD-GN-ER-501 [d]

[a] Geomatrix, 1996, *Probabilistic Seismic Hazard Analysis DOE Hanford Site, Washington,* WHC-SD-W236A-TI-002, Rev.1A, prepared for Westinghouse Hanford Company, Richland, Washington.

[b] DOE STD-1020-94, (1996, Change 1) *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, U.S. Department of Energy, Washington, D.C., 1996.

[c] DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98.

[d] HNF-SD-GN-ER-501, Rev. 1, "Natural Phenomena Hazards, Hanford Site, South-Central Washington", Westinghouse Hanford Company.

Figure 4-1

RPP-WTP DBE Horizontal Response Spectra
(0.50%, 2%, 3%, 4%, 5%, 7%, 10%, 12% Damping)

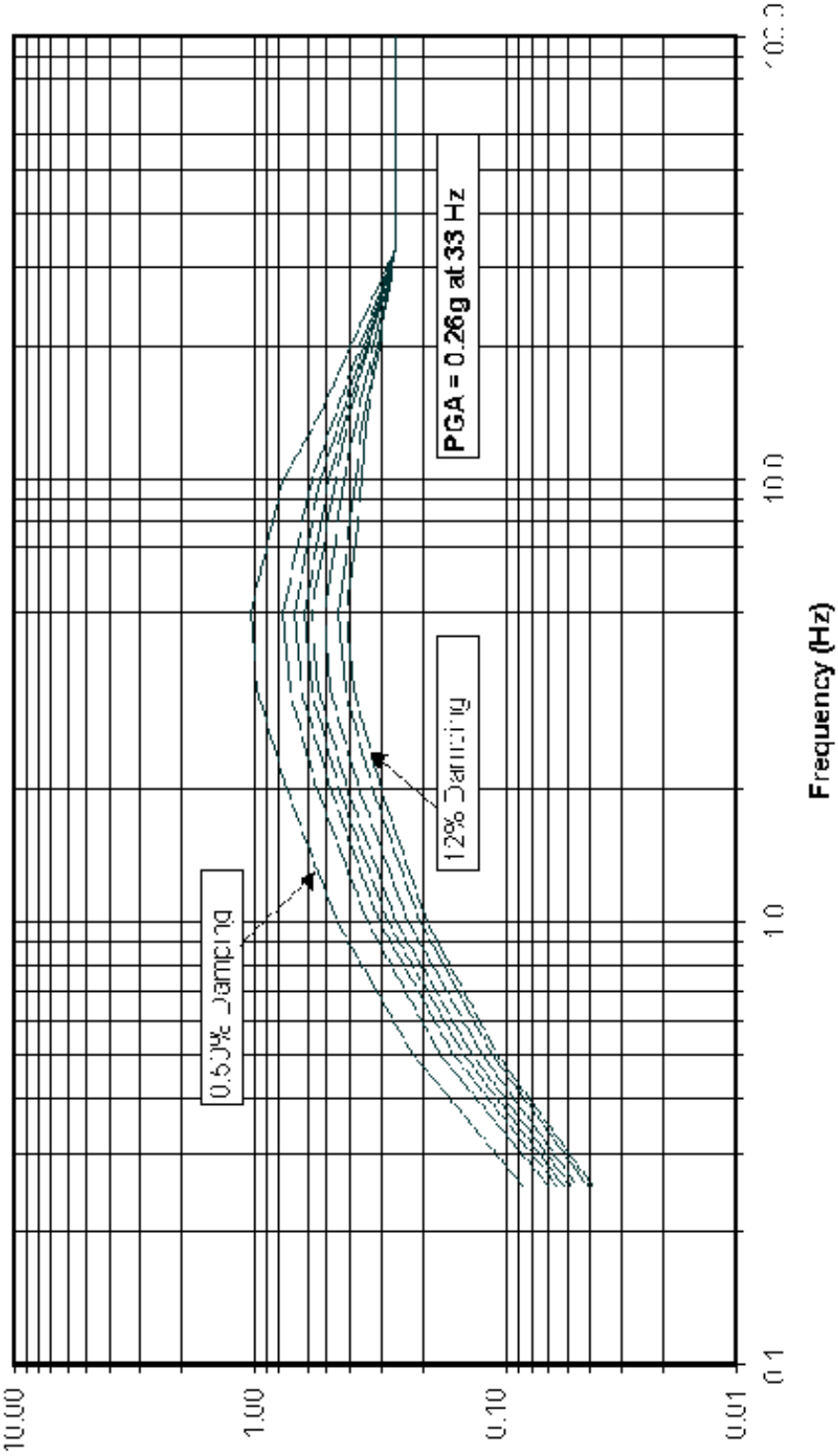
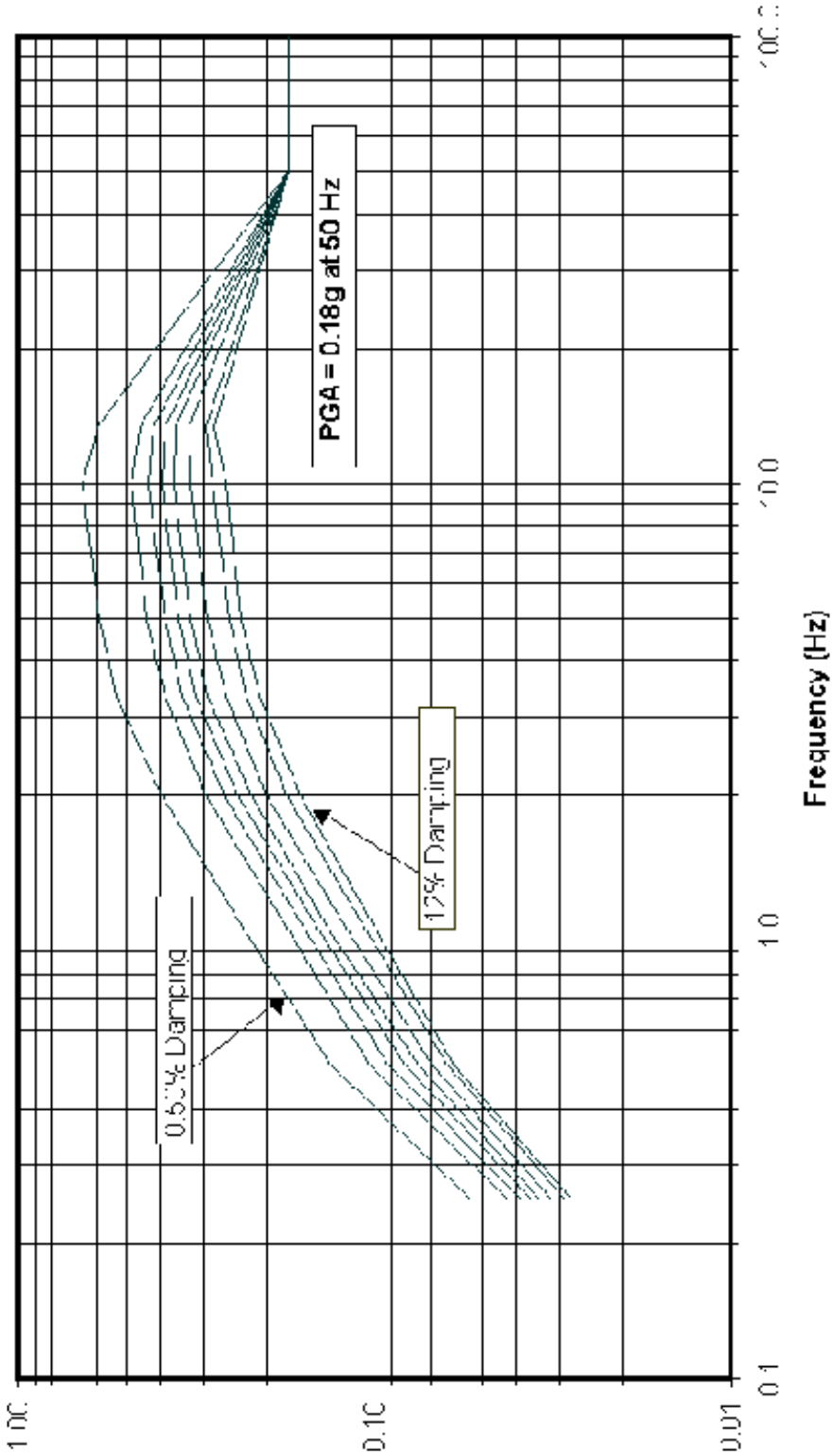


Figure 4-2

RPP-WTP DBE Vertical Response Spectra
(0.50%, 2%, 3%, 4%, 5%, 7%, 10%, 12% Damping)



Implementing Codes and Standards

ACI 349-01, *Code Requirements for Nuclear Safety-Related Concrete Structures*
ACI 349R-01, *Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures*
ACI 530-99, *Building Code Requirements for Masonry Structures and Commentary*
ANSI/AISC N690-94, *Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities*
ASCE 4-98, *Seismic Analysis of Safety-Related Nuclear Structures and Commentary*
ASCE 7-95, *Minimum Design Loads for Buildings and Other Structures*
DOE-STD 1020-94 (Change 1, 1996), *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*
IEEE 344-1987 (R1993), *Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*
1997, *UBC Uniform Building Code*
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix A, "Implementing Standard for Safety Standards and Requirements Identification"

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.1 - 4

This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) without NPH safety functions.

This criterion also addresses SSCs required to protect workers and members of the public from exposure to chemical hazards with an NPH safety function.

SSCs that may be important to the safety of the RPP-WTP shall be designed to withstand the effects of NPH such as earthquakes, wind, and floods. The SSCs included under this criterion are:

1. SSCs Important to Safety (either Safety Design Class or Safety Design Significant) that do not have an NPH safety function,
2. SSCs that are not Important to Safety and that have significant inventories of radioactive or hazardous materials but in amounts less than quantities that might lead to an Important to Safety designation, and
3. SSCs that are important to safety because of their function to protect workers and members of the public from exposure to chemical hazards.

These SSCs are designated Seismic Category III (SC-III) for earthquakes and Performance Category 2 (PC-2) for other NPH.

SSCs included under this criterion shall be designed to withstand the NPH loadings as provided in Table 4-2.

Table 4-2. Natural Phenomena Design Loads for SSCs without NPH Safety Functions

Hazard	Load	Source Document for Load
Seismic	Uniform Building Code [a], Static Force Procedure	DOE-STD-1020-94 [b]
Straight wind	91 mi/hr 3-second gust, at 33 ft above ground, Importance factor, I=1.00	DOE Newsletter [c]
Wind Missile	Not Applicable	DOE-STD-1020-94 [b]
Tornado and Tornado Missiles	Not Applicable	DOE-STD-1020-94 [b]
Volcanic ash	5 lb/ft^2	HNF-SD-GN-ER-501 [d]
Flooding	Dry site for river flooding Local Precipitation: 2.5 in. for 6 hours	HNF-SD-GN-ER-501 [d]
Snow	15.0 lb/ft^2 snow load	HNF-SD-GN-ER-501 [d]

[a] 1997, *Uniform Building Code,* International Conference of Building Officials, Whittier, California.

[b] DOE STD-1020-94, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, U.S. Department of Energy, Washington, D.C., Change 1, 1996.

[c] DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98

[d] HNF-SD-GN-ER-501, Rev. 1, "Natural Phenomena Hazards, Hanford Site, South-Central Washington", Westinghouse Hanford Company

Implementing Codes and Standards

ACI 318-99, *Building Code Requirements for Structural Concrete*
ACI 318R-99, *Commentary on Building Code Requirements for Structural Concrete*
AISC MO16-89, *Manual for Steel Construction - Allowable Stress Design, Ninth Edition*
ASCE 7-95, *Minimum Design Loads for Buildings and Other Structures*
DOE-STD 1020-94 (Change 1, 1996), *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*
1997, *UBC Uniform Building Code*
ACI 530-99, *Building Code Requirements for Masonry Structures and Commentary*
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix A, "Implementing Standard for Safety Standards and Requirements Identification"

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.1 - 5

Structures, systems, and components designated as Safety Design Class shall be appropriately protected against dynamic effects (e.g., the effects of missiles, pipe whipping, and discharging fluids) that may result from failures of moderate and high energy systems or other accident conditions.

In consideration of the need to protect structures, systems, and components which are designated as Safety Design Class from these dynamic effects, the failure of the moderate or high energy system need not be postulated to occur simultaneously with an accident unless the events are causally related.

Implementing Codes and Standards

ACI 349-01, *Code Requirements for Nuclear Safety-Related Concrete Structures*
ACI 349R-01, *Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures*
ANSI/AISC N690-94, *Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities*
ASCE 4-98, *Seismic Analysis of Safety-Related Nuclear Structures and Commentary*
ASCE 7-95, *Minimum Design Loads for Buildings and Other Structures*
DOE-STD 1020-94 (Change 1, 1996), *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98

Safety Criterion: 4.1 - 6

Adequate provisions for facility security and physical protection of structures, systems, and components Important to Safety shall be provided.

Implementing Codes and Standards

PL-W375-MG0004, Safeguards and Security Program Plan

Regulatory Basis

DOE/RL-96-0006 4.3.6.1 Security-Security

4.2 Confinement Design

Safety Criterion: 4.2 - 1

The facility shall be designed to retain the radioactive and hazardous material through a conservatively designed confinement system for normal operations, anticipated operational occurrences, and accident conditions. The confinement system shall protect the worker and public from undue risk of releases such that the radiological and chemical exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2

Regulatory Basis

DOE/RL-96-0006 4.1.1.4 Defense in Depth-Mitigation

Safety Criterion: 4.2 - 2

Important to Safety liquid and gaseous systems and components, including pressure vessels, tanks, heat exchangers, piping, and valves, shall be designed to retain their hazardous inventory such that the radiological and chemical worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 4.2 - 3

Codes and standards for Important to Safety vessels and piping should be supplemented by additional measures (such as erosion/corrosion programs and piping in-service inspections) to mitigate conditions arising that could lead to a release of radiological or chemical material that would exceed the worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI)
Document P001/2 Rules for the Design of Piping Systems
Document V001/2 Rules for the Design of Vessels

Regulatory Basis

DOE/RL-96-0006 4.2.2.4 Proven Engineering Practices/Margins-Codes and Standards

Safety Criterion: 4.2 - 4

Liquid and gaseous storage systems designated as Important to Safety shall have continuous monitoring to detect the loss or degradation of their safe storage function. As appropriate the following shall be monitored:

1. temperature; pressure; radioactivity in ventilation exhaust and liquid effluent streams
2. liquid levels
3. tank chemistry; condensate and cooling water
4. generation of flammable and explosive mixtures of gases

Implementing Codes and Standards

ANSI N42.18-1980 (Rev 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S12.13 PT 1-95 Performance Requirements, Combustible Gas Detectors

4.3 Engineered Safety Systems

Safety Criterion: 4.3 - 1

Engineered safety systems shall be designed (1) to initiate automatically the operation of appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided.

Implementing Codes and Standards

ANSI/ANS 58.8-1994 Time Response Design Criteria for Safety-Related Operator Actions
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries

Regulatory Basis

DOE/RL-96-0006 *4.1.1.5 Defense in Depth-Automatic Systems*

Safety Criterion: 4.3 - 2

When single failure protection is required, Important to Safety engineered safety systems shall be designed to assure that the effects of natural phenomena (including lightning), and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
NFPA 780-95 Standard for the Installation of Lightning Protection Systems
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.3 - 3

Important to Safety engineered safety systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components Important to Safety resulting from a common-cause or common-mode failure.

The protection system shall be designed to permit periodic testing of its functioning when the facility is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006 4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure

Safety Criterion: 4.3 - 4

Important to Safety instrumentation and controls shall be provided to monitor variables and systems and control systems and components over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate public and worker safety by compliance to the standards of Safety Criteria 2.0-1 and 2.0-2, including those variables and systems that can affect the performance of Important to Safety facility conditions. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The instrumentation and controls provided shall provide the ability to detect off normal conditions, mitigate accidents, and place the facility in a safe state.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations
ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries

Regulatory Basis

DOE/RL-96-0006 4.1.1.3 Defense in Depth-Control
DOE/RL-96-0006 4.2.6.2 Human Factors-Instrumentation and Control Design

Safety Criterion: 4.3 - 5

When single failure protection is required, Important to Safety protection systems shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits

Safety Criterion: 4.3 - 6

The possibility of human error in facility operations shall be taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions and by providing means for detecting and correcting or compensating for error. The parameters to be monitored in control areas shall be selected and their displays arranged to ensure operators have clear and unambiguous indication of the status of the facility. The parameters and displays shall facilitate monitoring and the initiation and operation of systems designated as Important to Safety.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 1023-88 Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006	*4.1.1.6*	*Defense in Depth-Human Aspects*
DOE/RL-96-0006	*4.2.6.1*	*Human Factors-Human Error*
DOE/RL-96-0006	*4.2.6.2*	*Human Factors-Instrumentation and Control Design*
DOE/RL-96-0006	*4.2.6.3*	*Human Factors-Safety Status*

Safety Criterion: 4.3 - 7

The control room or control area shall be designed to permit occupancy and actions to be taken to monitor the facility safely during normal operations, and to provide safe control of the facility for anticipated operational occurrences and accident conditions. If credit is taken for operator action to satisfy the accident exposure standards of Safety Criteria 2.0-1 and/or 2.0-2, adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body gamma and 30 rem beta skin for the duration of the accident. For occurrences and accidents involving chemical release, provisions shall be made such that the operator exposure does not exceed the worker exposure standards of 29 CFR 1910.120 for emergency exposure.

Consideration shall also be given to accidents at nearby facilities if operator action is required to safely control the processes and bring them to a safe state.

The need for an alternate system that would allow the processes to be placed in a safe state in the event the primary control area is uninhabitable shall be evaluated.

Implementing Codes and Standards

ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
ASME N510-1989 (Rev 1995) Testing of Nuclear Air Cleaning Systems
NUREG-0800 Standard Review Plan, Section 6.4, Section II, Items 1-5.
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006	*4.2.4.1 Emergency Preparedness-Support Facilities*
DOE/RL-96-0006	*4.2.6.2 Human Factors-Instrumentation and Control Design*
29 CFR 1910.120	*Hazardous Waste Operations and Emergency Response*

4.4 Electrical and Mechanical Systems

Safety Criterion: 4.4 - 1

A list of electric and mechanical components designated as Important to Safety shall be prepared and maintained. The list shall include:

(1) The performance specifications for normal operation and under conditions existing during and following accidents.

(2) The load, pressure, voltage, frequency, and other characteristics, as appropriate, for which the performance specified can be ensured.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 4.4 - 2

Structures, systems, and components Important to Safety shall be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning shall be considered in design and qualification.

Implementing Codes and Standards

10 CFR 50.49 Environmental qualification of electric equipment important to safety for nuclear power
IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006 *4.2.2.3 Proven Engineering Practices/Margins-Safety System Design and Qualification*

Safety Criterion: 4.4 - 3

This Criterion has been deleted.

Safety Criterion: 4.4 - 4

Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.

Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin. Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended operating life.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI)

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Regulatory Basis

DOE/RL-96-0006 4.2.7.1 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Reliability

DOE/RL-96-0006 4.2.7.2 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Availability, Maintainability, and Inspectability

Safety Criterion: 4.4 - 5

Each air treatment system designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and confinement capabilities to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) its safety function can be accomplished, assuming a single failure.

The use of alternate equipment may be considered to satisfy the single failure requirement.

Implementing Codes and Standards

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 6

Each air treatment system designated as Safety Design Class shall be designed to ensure its operability under normal and accident conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) the structural and leaktight integrity of its components

(2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves

(3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of associated systems

Implementing Codes and Standards

ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
UL 586-90 High Efficiency Particulate Air Filter Units, Seventh Edition

Safety Criterion: 4.4 - 7

Each air treatment system designated as Safety Design Significant shall be designed to ensure its operability under normal conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) the structural and leaktight integrity of its components

(2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves

(3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system

Implementing Codes and Standards

UL 586-90 High Efficiency Particulate Air Filter Units, Seventh Edition

Safety Criterion: 4.4 - 8

Ventilation systems and off-gas systems must be provided where necessary to control radiological and chemical material releases and the generation of flammable and explosive gases during normal and off-normal conditions.

Implementing Codes and Standards

ARI 670-90 Fans and Blowers
ASME N509-89 Nuclear Power Plant Air Cleaning Units and Components
ASME N510-1989 (Rev 1995) Testing of Nuclear Air Cleaning Systems
ASME PTC 11-84 Performance Test Codes, Fans
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 1002

Safety Criterion: 4.4 - 9

An onsite electric power system and an offsite electric power system shall be provided to permit functioning of systems designated as Safety Design Class. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure Safety Design Class functions are maintained in the event of postulated accidents. The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their specified safety functions assuming a single failure.

Implementing Codes and Standards

IEEE 308-91 Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 450-1995 Practice for Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Generating Stations and Substations
IEEE 484-1996 Recommended Practice for Installation Design and Installation of Large Lead Storage Batteries for Generating Stations and Substations
IEEE 485-1983 Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations
IEEE 628-1987 Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations
IEEE 741-1990 Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations
IEEE 946-1992 Design of Safety-Related DC Auxiliary Power Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 10

Physical and electrical separation shall be provided between diverse or redundant Safety Design Class electrical systems. Associated circuits should be avoided.

Implementing Codes and Standards

IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 628-1987 Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 11

Electric power systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to periodically test:

(1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses

(2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of the offsite power system and the onsite power system

Implementing Codes and Standards

IEEE 338-1987 Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 12

Electric power systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to periodically test:

(1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses

(2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE 387-1995 Standard Criteria for Diesel-Generator Units Applied as Standby Power Generating Stations
NFPA 70-1996 National Electric Code

Safety Criterion: 4.4 - 13

Instrument air systems designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 14

Instrument air systems designated as Safety Design Class that provide air to a non-Safety Design Class air system shall be provided with adequate isolation such that failure of the non-Safety Design Class portion of the system will not prevent the Safety Design Class portion from performing its specified safety function.

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems

Safety Criterion: 4.4 - 15

Instrument air systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic pressure and functional testing to assure:

(1) air quality

(2) the structural integrity of its components

(3) the operability and the performance of the active components of the system

(4) the operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources

Implementing Codes and Standards

ANS 59.3-1992 Nuclear Safety Criteria for Control Air Systems
ASME B31.3-96 Process Piping
ASME PTC 9-70 Performance Test Codes, Displacement Compressors, Vacuum Pumps and Blowers
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 16

Instrument air systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic pressure and functional testing to assure:

(1) air quality

(2) the structural integrity of its components

(3) the operability and the performance of the active components of the system

(4) the operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME PTC 9-70 Performance Test Codes, Displacement Compressors, Vacuum Pumps and Blowers
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
ISA S7.0.01-1996 Quality Standard for Instrument Air

Safety Criterion: 4.4 - 17

Instrument air systems supplying air to Important to Safety equipment shall provide clean, dry, and oil free air to this equipment. The instrument air shall be free of all corrosive and hazardous gases which may be drawn into the system.

Implementing Codes and Standards

ISA S7.0.01-1996 Quality Standard for Instrument Air

Safety Criterion: 4.4 - 18

Cooling water systems designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

Implementing Codes and Standards

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Generating Stations

Safety Criterion: 4.4 - 19

Cooling water systems designated as Safety Design Class shall be designed to ensure their operability under normal and accident conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) Long term corrosion and/or organic fouling that could degrade system performance is detected. This shall include consideration of the impacts of organic fouling on heat exchanger performance.

(2) The potential for radioactive leakage into and out of the system and to the environment is minimized.

(3) The structural and leaktight integrity of its components.

(4) The operability and the performance of the active components of the system.

(5) The operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

Safety Criterion: 4.4 - 20

Cooling water systems designated as Safety Design Significant shall be designed to ensure their operability under normal conditions. The design shall permit appropriate periodic inspection and pressure and functional testing to assure:

(1) Long term corrosion and/or organic fouling that could degrade system performance is detected. This shall include consideration of the impacts of organic fouling on heat exchanger performance.

(2) The potential for radioactive leakage into and out of the system and to the environment is minimized.

(3) The structural and leaktight integrity of its components.

(4) The operability and the performance of the active components of the system.

(5) The operability of the system as a whole and, under conditions as close to design as practical, including operation of applicable portions of the protection system.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
NFPA 214-96 Standard on Water-Cooling Towers
TEMA B, C, or R TEMA Class “B”, “C”, or “R” Heat Exchangers Mechanical Standards

Safety Criterion: 4.4 - 21

Safety Design Class motor operated valves shall be specified to ensure operability against the maximum differential pressure that might occur while performing their specified accident prevention or mitigation safety function at the minimum specified terminal voltage. Consideration for mis-positioned valves is not a requirement in determining the maximum differential pressure.

Periodic testing of Safety Design Class motor operated valves shall be performed to confirm their ability to perform their specified accident prevention or mitigation safety function.

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE 382-1985 Standard for Qualification of Actuators for Power Operated Valve Assemblies with Safety-Related Functions for Nuclear Power Plants

4.5 Fire Protection

Safety Criterion: 4.5 - 1

Two reliable and separate water supplies of adequate capacity for fire suppression shall be provided.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 2

Buildings containing a significant quantity of radioactive and/or hazardous material shall be constructed of noncombustible or fire-resistive material, where appropriate.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 3

Confinement of the fire to its origin should be achieved through passive barriers and by activating systems such as fire and smoke dampers, exhaust fans, and drainage pumps to prevent migration of gases, hot combustion products, and flammable liquids outside the fire area.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 4

Automatic fire extinguishing systems shall be included in all areas subject to loss of Safety Design Class systems, significant life safety hazards, or unacceptable program interruption, unless the Fire Hazards Analysis dictates otherwise.

As determined by the Fire Hazards Analysis special hazards shall be provided with additional fixed protection systems.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 5

Redundant Safety Design Class systems and components should be in separate fire areas.

Redundant, primary and secondary, fire protection systems shall be provided in areas where Safety Design Class systems and components are vulnerable to fire damage and where no redundant safety capability exists outside of the fire area.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 6

The design shall incorporate life safety features including means to notify and evacuate building occupants in the event of a fire, such as a fire detection or fire alarm system and illuminated, protected egress paths.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 7

The facility shall include a fire detection system to detect the presence of a fire and activate alarm systems so that measures for confinement and suppression of the fire and personnel evacuation may start promptly. The detection system shall include a means to summon the Hanford Site fire department. The system shall be capable of operation without offsite power.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 8

The facility shall include physical access and appropriate equipment to facilitate effective intervention by the Hanford Site fire department, such as an interior standpipe system.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 9

The facility design shall provide for the prevention of accidental release of significant quantities of contaminated products of combustion and fire fighting water to the environment. This can be provided by such features as ventilation control and filter systems, curbs, dikes, and holding ponds.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 10

Fire and related hazards that are unique to the facility and are not addressed by industry codes and standards shall be protected by isolation, segregation, or use of special fire control systems, such as inert gas or explosion suppression, as determined by the Fire Hazards Analysis.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 11

Fire protection systems shall be designed, and/or systems and components protected, such that its/their inadvertent operation, inactivation, or failure of structural stability will not result in the loss of a Safety Design Class function.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 12

The fire protection program shall establish the fire protection policy for the protection of the facility and the procedures, equipment, and personnel required to implement the program. The program shall have the following objectives:

(1) To prevent fires from starting

(2) To detect early, control and extinguish promptly those fires that do occur

(3) To provide protection for Safety Design Class SSCs

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 13

The fire protection program and features shall be characterized by a level of fire protection that is sufficient to fulfill the requirements of the best protected class of industrial risks ("Highly Protected Risk" or "Improved Risk") and shall be provided protection to achieve "defense-in-depth."

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 14

A fire protection program shall be developed that will minimize the potential for the occurrence of a fire or explosive threat and, should such an event occur, the program will limit:

(1) Radiological and hazardous releases from the facility

(2) The threat to the health and safety of facility workers

(3) Interruption of the facility mission to process tank waste

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 15

The fire protection program will include:

(1) organization, training, and responsibilities of the fire protection staff, including a trained and equipped emergency services organization

(2) inspection, testing, and maintenance of all fire protection systems by personnel properly qualified by experience and training in fire protection systems

(3) surveillance to ensure that fire barriers are in place and that fire suppression systems and components are operable

(4) training of all employees in basic fire safety

(5) periodic performance of fire drills

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 16

The fire protection program will include a plan to identify, prioritize, and monitor the status of fire protection-related appraisal findings/recommendations until final resolution is achieved. When final resolution will be significantly delayed, appropriate interim compensatory measures shall be implemented to minimize the fire risk.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 17

The fire protection program shall ensure fire protection requirements are documented and incorporated in the plans and specifications for all new facilities and for significant modifications of existing facilities. This includes a documented review by a qualified fire protection engineer of plans, specifications, procedures, and acceptance tests.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 18

The fire protection program shall include a comprehensive, documented fire protection self-assessment program, which includes all aspects (program and facility) of the fire protection program.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 19

Administrative controls shall be established to minimize fire hazards. These shall include procedures to:

(1) govern the handling and storage of combustible and flammable materials

(2) govern the handling of transient fire loads in buildings containing Safety Design Class SSCs

(3) designate staff members responsible for fire protection review of proposed work activities

(4) govern the use of ignition sources (e.g., through the use of a flame permit system)

(5) control the expedient removal of combustibles resulting from work activities

(6) establish compensatory controls for activities which may result in the impairment of fire prevention and/or mitigation features

(7) maintain periodic housekeeping inspections to ensure continued compliance with these administrative controls

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 20

A Fire Hazard Analysis (FHA) of the facility shall be performed. Such a systematic analysis shall divide the facility into "fire areas" and evaluate the fire safety of each area and of the facility as a whole. The analysis shall, for each fire area:

(1) Account for all radioactive, hazardous, and combustible materials, including estimates of their heat content

(2) Describe the processes performed and their potential for fire or explosion

(3) Account for the sources of heat and flame

(4) List the fire detection and suppression equipment

(5) Consider credible fire scenarios and evaluate the adequacy of the fire protection measures

In addition, the FHA shall consider other buildings or installations close to process buildings that contain flammable, combustible, or reactive liquid or gas storage.

The FHA shall confirm that the facility can be placed in a safe state during and after all credible fire and explosion conditions.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
DOE-STD-1066-97 Fire Protection Design Criteria
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 21

The fire protection program shall be under the direction of an individual who has been delegated authority commensurate with the responsibilities of the position and who has available staff knowledgeable in both fire protection and nuclear safety.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 22

The facility should have on file, and ready to use, a Pre-Fire Plan. The Pre-Fire Plan should assign individual and alternate responsibilities for responding to a fire alarm or call; assessing the situation, suppressing incipient fires, assembling the emergency service organization, personnel evacuation, orderly shutdown of processes, and safeguarding (if necessary) and control of radioactive and hazardous material.

The plan should clearly indicate, preferably with the help of site plans and drawings, the locations of the fire department-compatible connections and fire-fighting equipment, such as portable extinguishers, automatic fire suppression systems, sectional valves, standpipes, hydrants, and hoses. It should also indicate the areas of concentrations of combustibles, storage of flammable and combustible liquids, and areas where use of water for fire suppression is restricted because of nuclear criticality or other concerns.

The Pre-Fire Plan should be prepared in consultation and coordination with the Hanford Site fire department. The Hanford Site fire department personnel should be given familiarization tours of the facility at least once a year.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.5 - 23

Hot work permits shall be issued for hot work operations conducted in or near the facility. The permit shall document that applicable fire prevention and protection requirements have been implemented prior to beginning the hot work operations; it shall indicate the date(s) authorized for hot work; and identify the object on which hot work is to be performed. The permit shall be kept on file until completion of the hot work operations.

Implementing Codes and Standards

DOE G-440.1 Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Regulatory Basis

DOE/RL-96-0006 5.2.8 Hot Work Control

5.0 Radiation Protection

Safety Criterion: 5.0 - 1

A Radiation Protection Program (RPP) compliant with 10 CFR 835 shall be developed and submitted for approval to DOE.

The RPP-WTP Radiological Controls Program shall address all items in 10 CFR 835 and the additional Safety Criteria provided in SRD Volume II Sections 5.1 and 5.2.

Implementing Codes and Standards

DOE G 441.1-1, Management and Administration of Radiation Protection Programs Guide

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 101(a-f)
DOE/RL-96-0006 4.2.3.1 Radiation Protection-Radiation Protection Practices
DOE/RL-96-0006 4.3.2.1 Radiation Protection-Radiation Practices
DOE/RL-96-0006 4.3.2.2 Radiation Protection-Procedures and Monitoring

5.1 Occupational Radiation Protection

Safety Criterion: 5.1 - 1

This safety criterion has been deleted.

Safety Criterion: 5.1 - 2

A respiratory protection program shall be established that includes:

(1) Use of respiratory protection equipment, including equipment used as emergency devices, that is tested and certified or had certification extended by the National Institute for Occupational Safety and Health/Mine Safety and Health Administration (NIOSH/MSHA).

(2) Air sampling sufficient to identify the potential hazard, permit proper equipment selection, and estimate exposures.

(3) Surveys and bioassays, as appropriate, to evaluate actual intakes.

(4) Testing of respirators for operability immediately prior to each use.

(5) Written procedures regarding selection, fitting, issuance, maintenance, and testing of respirators, including testing for operability immediately prior to each use; supervision and training of personnel; monitoring, including air sampling and bioassays; and recordkeeping.

(6) Determination by a physician prior to the initial fitting of respirators, and either every 12 months thereafter or periodically at a frequency determined by a physician, that the individual user is medically fit to use the respiratory protection equipment.

(7) A written policy statement on respirator usage covering:

(i) The use of process or other engineering controls, instead of respirators.

(ii) The routine, nonroutine, and emergency use of respirators.

(iii) The periods of respirator use and relief from respirator use. Each respirator user will be informed that they may leave the area at any time for relief from respirator use in the event of equipment malfunction, physical or psychological distress, procedural or communication failure, significant deterioration of operating conditions, or any other conditions that might require such relief.

(8) Use of equipment within limitations for type and mode of use and provision for proper visual, communication, and other special capabilities (such as adequate skin protection) when needed.

(9) Notification to the Regulator, in writing, at least 30 days before the date that respiratory protection equipment is first used to protect workers from airborne radioactivity.

Implementing Codes and Standards

ANSI Z-88.2-1992 American National Standard for Respiratory Protection

Safety Criterion: 5.1 - 3
This safety criterion has been deleted.

Safety Criterion: 5.1 - 4
This safety criterion has been deleted.

Safety Criterion: 5.1 - 5
This safety criterion has been deleted.

Safety Criterion: 5.1 - 6
This safety criterion has been deleted.

Safety Criterion: 5.1 - 7
This safety criterion has been deleted.

5.2 Occupational Radiation Protection Design

Safety Criterion: 5.2 - 1

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 2

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 3

This Safety Criterion has been deleted

Safety Criterion: 5.2 - 4

This Safety Criterion has been deleted

5.3 Environmental Radiation Protection

Safety Criterion: 5.3 - 1

An Environmental Radiological Protection Program shall be prepared and submitted to the regulator.

The Environmental Radiological Protection Program (ERPP) shall address the following elements, as appropriate:

(1) the identity of existing and anticipated types of activities and areas of the site subject to the ERPP

(2) the measures to be used to implement the ERPP

(3) the methods to be used to monitor, report, and record compliance with the ERPP

(4) models and methods used for dose assessment including bioaccumulation and dose-conversion factors

(5) an As Low As is Reasonably Achievable (ALARA) Program

(6) effluent and environmental monitoring including:

- (i) sources of airborne emissions
- (ii) sources of discharges in liquid waste streams
- (iii) effluent monitoring
- (iv) environmental surveillance
- (v) meteorological data acquisition
- (vi) pre-operational evaluation

(7) ground water protection

(8) radiological protection in the management of radioactive waste

(9) controls on the release of materials

(10) property containing residual radioactive materials

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specifications with guidance for use

Regulatory Basis

DE-AC06-96RL13308 Part I Section C.5 Table S4-1
DOE/RL-96-0006 4.3.2.1 Radiation Protection-Radiation Practices
DOE/RL-96-0006 4.3.2.2 Radiation Protection-Procedures and Monitoring

Safety Criterion: 5.3 - 2

The ALARA Program shall ensure that releases of radioactive materials to the environment and exposures to the public during normal operations shall be kept ALARA and within prescribed limits.

Implementing Codes and Standards

DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features
WAC 173-480 Ambient Air Quality Standards and Emission Limits for Radionuclides Location: Part 050 (1)

Safety Criterion: 5.3 - 3

A waste management program shall ensure compliance with all applicable laws and regulations. The waste management program shall also ensure that the radiological impact to the general public and environment due to radioactive wastes arising from RPP-WTP operation shall be ALARA.

Implementing Codes and Standards

IAEA Safety Series No. 50-SG-011, Operational Management for Radioactive Effluents and Wastes Arising in Nuclear Power Plants.
ANSI/ISO-14001-1996, Environmental Management Systems - Specifications with guidance for use

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features

Safety Criterion: 5.3 - 4

Equipment shall be designed and installed to monitor and maintain control over radioactive materials in gaseous and liquid effluents produced during normal operations, including anticipated operational occurrences.

Implementing Codes and Standards

40 CFR 52 Appendix E Performance Specifications and Specification Test Procedures for Monitoring Systems for Effluent Stream Gas Volumetric Flow Rate
40 CFR 60 Appendix A, Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17
ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N42.18-1980 (R 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
ANSI N323 Radiation Protection Instrumentation Test and Calibration
ASME/ANSI AG-1, Code on Nuclear Air and Gas Treatment
ASME/ANSI N509, Nuclear Power Plant Air-Cleaning Units and Components
ASME/ANSI N510, Testing of Nuclear Air Cleaning Systems
ACGIH 1988, Industrial Ventilation, A Manual of Recommended Practice, 20th Edition, American Conference of Governmental Industrial Hygienists.
ERDA 76-21, Nuclear Air Cleaning Handbook

Regulatory Basis

DOE/RL-96-0006 3.2 Radiation Protection Objective
DOE/RL-96-0006 4.2.3.2 Radiation Protection-Radiation Protection Features
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075
WAC 246-247 Radiation Protection - Air Emissions Location: Part 110

Safety Criterion: 5.3 - 5

All new construction and significant modifications of air emission units shall utilize best available radionuclide control technology (BARCT).

Implementing Codes and Standards

WAC 246-247-120 Appendix B BARCT Compliance Demonstration
ASME/ANSI AG-1, Code on Nuclear Air and Gas Treatment
ASME/ANSI N509, Nuclear Power Plant Air-Cleaning Units and Components
ASME/ANSI N510, Testing of Nuclear Air Cleaning Systems
ANSI N13.1, Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N42.18, Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents
ERDA 76-21, Nuclear Air Cleaning Handbook
ACGIH 1988, Industrial Ventilation, A Manual of Recommended Practice, 20th Edition, American Conference of Governmental Industrial Hygienists.
40 CFR 60 Appendix A, Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17

Regulatory Basis

WAC 173-480 Ambient Air Quality Standards and Emission Limits for Radionuclides Location: Part 060
WAC 246-247 Radiation Protection - Air Emissions Location: Part 040 (3)

Safety Criterion: 5.3 - 6

Activities shall be conducted in such a manner that no radioactive material is discharged into sanitary sewers. Exempt from this Safety Criterion are trace radioactive materials present in:

(1) readily soluble waste such as kitchen waste from breakrooms, custodial cleaning solutions, or other materials of similar non-RPP-WTP process origin

(2) biological waste (solid and liquid human waste) which is readily dispersed in water

Also exempt from this Safety Criterion are excreta from individuals undergoing medical diagnosis or therapy with radioactive materials.

Implementing Codes and Standards

IAEA Safety Series No. 50-SG-011, Operational Management for Radioactive Effluents and Wastes Arising in Nuclear Power Plants.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.2*	*Radiation Protection-Radiation Protection Features*

Safety Criterion: 5.3 - 7

Liquid discharges from the facility, other than sanitary sewer discharges, shall comply with ALARA process requirements, be treated by the best available technology, and not result in release of settleable solids to surface waters for streams exceeding 5 pCi/g for alpha-emitting radionuclides, and/or 50 pCi/g for beta-emitting radionuclides.

Note: The RPP-WTP design does not include provisions for liquid waste discharges, other than sanitary sewer discharges. Therefore, Implementing Codes and Standards are not required. If the RPP-WTP design changes such that liquid discharges result, an SRD revision will be prepared.

Safety Criterion: 5.3 - 8

Controls on the release of materials and property containing residual radioactive material shall be established.

Implementing Codes and Standards

10 CFR 835, Occupational Radiation Protection, Appendix D (ad hoc)

Note: The Appendix D values will be used as surface contamination criteria for determining the suitability of releasing material from radiologically controlled areas. These criteria are not applicable to materials potentially contaminated throughout their volume. Because the RPP-WTP process feed is a mixed waste, any items that are determined to be contaminated, will also be assumed to be a mixed waste (i.e., containing a State of Washington dangerous waste). Rather than determine the quantities of dangerous wastes present, these materials will be disposed of as mixed wastes.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.1*	*Radiation Protection-Radiation Protection Practices*

5.4 Environmental Radiological Monitoring

Safety Criterion: 5.4 - 1

Each source shall have capability for independent effluent emission testing as follows:

(1) Sampling ports adequate for test methods applicable to each source

(2) Safe sampling platform(s)

(3) Safe access to sampling platform(s)

(4) Utilities for sampling and testing equipment

(5) Any other facilities deemed necessary to safely and properly test a source

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 13
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (10)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (9)

Safety Criterion: 5.4 - 2

Nonpoint and fugitive emissions of radioactive material shall be monitored.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (8)

Safety Criterion: 5.4 - 3

Direct measurements shall be made, to the extent practicable, to obtain information characterizing source terms, exposures, exposure modes, and other information needed in evaluating doses.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

WAC 246-221 Radiation Protection Standards Location: 070 (1)

Safety Criterion: 5.4 - 4

When the effluents from a single source, or from two or more sources subject to the same emission standards, are combined before being released to the atmosphere, a monitoring system shall be installed on each effluent or on the combined effluent. If two or more sources are not subject to the same emission standards, a separate monitoring system shall be installed on each effluent. If the applicable standard is a mass emission standard and the effluent from one source is released to the atmosphere through more than one point, a monitoring system shall be installed at each emission point.

Implementing Codes and Standards

ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 14 (d)

Safety Criterion: 5.4 - 5

Equipment and procedures used for the continuous monitoring of radioactive air emissions shall conform, to applicable guidance.

Implementing Codes and Standards

40 CFR 52 Appendix E Performance Specifications and Specification Test Procedures for Monitoring Systems for Effluent Stream Gas Volumetric Flow Rate
40 CFR 60 Appendix A, Test Methods 1, 1a, 2, 2a, 2c, 2d, 4, 5,and 17
40 CFR 61 Appendix B, Test Method 114
ANSI N13.1-1969 (R 1993) Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
ANSI N323 Radiation Protection Instrumentation Test and Calibration
ANSI N42.18-1980 (R 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (2)

Safety Criterion: 5.4 - 6

Computer codes or procedures used to determine the offsite total effective dose equivalent from airborne emissions shall be EPA approved.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (2)

Safety Criterion: 5.4 - 7

Compliance with the annual dose limit for individual members of the public (100 mrem/yr from all sources) shall be shown by:

(1) Demonstrating by measurement or calculation that the total effective dose equivalent to the individual likely to receive the highest dose from the operation does not exceed the annual dose limit; or

(2) Demonstrating that:

(a) The annual average concentrations of radioactive material released in gaseous and liquid effluents at the boundary of the unrestricted area do not exceed the values specified in Table II of WAC246-221-290.

(b) If an individual were continuously present in an unrestricted area, the dose from external sources would not exceed 0.002 rem in an hour and 0.05 rem in a year.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 93
WAC 246-221 Radiation Protection Standards Location: 070 (2)
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (1)

Safety Criterion: 5.4 - 8

Compliance with the public air emission standard shall be determined by calculating the highest effective dose equivalent to any member of the public at any offsite point where there is a residence, school, business or office.

The determination of compliance shall include all radioactive air emissions resulting from routine and nonroutine operations for the past calendar year.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 94
WAC 246-247 Radiation Protection - Air Emissions Location: Part 085 (3)

Safety Criterion: 5.4 - 9

Records sufficient to demonstrate compliance with the dose limit for individual members of the public shall be maintained. Records must document the source of input parameters including the results of all measurements upon which they are based, the calculations and/or analytical methods used to derive values for input parameters, and the procedure used to determine compliance. This documentation should be sufficient to allow an independent auditor to verify the accuracy of the determination made concerning the facility's compliance.

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with Guidance for Use

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 95
WAC 246-247 Radiation Protection - Air Emissions Location: Part 080

Safety Criterion: 5.4 - 10

An environmental surveillance program shall be developed and implemented to include:

(1) Meteorological data acquisition (Note 1)

(2) Pre-operational evaluation (Note 2)

(3) Near-Facility Monitoring (Note 3)

(4) Ground Water Protection (Note 4)

Implementing Codes and Standards

ANSI/ISO-14001-1996, Environmental Management Systems - Specification with guidance for use

IAEA Safety Series No 41, *Objectives and Design of Environmental Monitoring Programmes for Radioactive Contaminants*

Notes:

1. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-22 between DOE and BNFL Inc. for Air Emissions,* Table 2 states that DOE will maintain the Hanford Site Air Operating Permit (AOP) and provide access to meteorological data.
2. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-09 Between DOE and BNFL Inc. for Land Siting,* Table 1, describes specific interfaces responsibilities for the RPP-WTP contractor and for the DOE. Item 12 of the table requires that the RPP-WTP contractor perform any additional site characterization work beyond that which was performed by the DOE. The RPP describes the plans and measures for compliance with the survey and contamination control requirements of 10 CFR 835.
3. As described in BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-22 between DOE and BNFL Inc. for Air Emissions,* DOE will continue to operate site and near-facility monitoring networks in the vicinity of the RPP-WTP site. Additional monitoring which is required will be provided by the RPP-WTP contractor. If additional monitoring is required, it will be performed consistent with the Hanford Site near-facility monitoring program for inclusion in site annual reports (example, HNF-EP-0573-6, *Hanford site Near-Facility Environmental Monitoring Annual Report, Calendar Year 1997*).
4. BNFL-5193-ID-03, *Interface Control Document*, Revision 2, *ICD-09 between DOE and BNFL Inc. for Land Siting,* Section 3.3, Ground Water Monitoring Wells, states that that the DOE will "…close groundwater monitoring well E25-32 prior to the start of site work…" There is no liquid discharge to the environment from RPP-WTP operations. Transfer piping to the Effluent Treatment Facility is by means of a three-inch pipe encased in a 6-inch pipe. Potential leakage from the transfer pipe is contained, and collected by the outer pipe. Accidental release of the inner pipe contents would be detected by the transfer pipe leak detection equipment. If both inner and outer pipes failed, such leakage could result in soil contamination which would be remediated prior to any contamination reaching the ground water.

Regulatory Basis

DOE/RL-96-0006	*3.2*	*Radiation Protection Objective*
DOE/RL-96-0006	*4.2.3.1*	*Radiation Protection-Radiation Protection Practices*

6.0 Startup

Safety Criterion: 6.0 - 1

A pre-operational testing program shall be established and followed to demonstrate that Important to Safety structures, systems and components have been properly constructed and can perform their specified functions. The program shall provide for the detection, tracking, and correction of deficiencies.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.1 Pre-Operational Testing-Testing Program

Safety Criterion: 6.0 - 2

Procedures for normal facility and systems operation and for functional tests to be performed during the operating phase shall be validated as part of the pre-operational testing program.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.2 Pre-Operational Testing-Operational Systems and Functional Testing Procedures Validation

Safety Criterion: 6.0 - 3

During pre-operational testing, detailed diagnostic data shall be collected on systems and components designated as Important to Safety and the initial operating parameters of the systems and components shall be recorded.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.14 Startup Testing
- Section: 3.14 Startup Testing and Operation
- Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.3 Pre-Operational Testing-Safety Systems Data

Safety Criterion: 6.0 - 4

During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components designated as Important to Safety shall be determined and documented. Operating points shall be adjusted to conform to values in the design basis. Training procedures and limiting conditions for operation shall be modified, if necessary, to accurately reflect the operating characteristics of the systems and components as built.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 3.14 Startup Testing and Operation
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.2.8.4 Pre-Operational Testing-Design Operating Characteristics

Safety Criterion: 6.0 - 5

A pre-startup safety review shall be performed. The pre-startup safety review shall confirm that, prior to the introduction of radioactive or process chemicals considered to pose a hazard to a process, construction and equipment is in accordance with design specifications; safety, operating, maintenance, and emergency procedures are in place and are adequate; a process hazard analysis has been performed and recommendations have been resolved or implemented before startup; and training of each employee involved in operating a process has been completed.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 4.3.1.4 Conduct of Operations-Readiness
DOE/RL-96-0006 5.2.6 Pre-startup Safety Review

7.0 Management and Operations

Safety Criterion: 7.0 - 1

Normal operations shall be conducted in accordance with approved operational safety requirements and in strict accordance with administrative and procedural controls.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.13 Procedures
Section: 5.6.1 Procedure Development

Regulatory Basis

DOE/RL-96-0006 4.3.1.2 Conduct of Operations-Normal Operations
DOE/RL-96-0006 5.1.3 Process Safety Responsibility

Safety Criterion: 7.0 - 2

Normal operation, including anticipated operational occurrences, maintenance, and testing, shall be controlled so that facility and system variables remain within their normal operating ranges and the frequency of demands placed on Important to Safety structures, systems, and components are small.

Implementing Codes and Standards

Regulatory Basis

DOE/RL-96-0006 4.1.1.3 Defense in Depth-Control

Safety Criterion: 7.0 - 3

The operating organizations shall become and remain familiar with the features and limitations of components included in the design of the facility. They shall obtain appropriate input from the design organization on pre-operational testing, operating procedures, and the planning and conduct of training.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 1.3.15 Operations

Regulatory Basis

DOE/RL-96-0006 4.1.5.2 Configuration Management-Contractor Design Knowledge

Safety Criterion: 7.0 - 4

The assignment and subdivision of responsibility for safety within the contractor's organization shall be kept well defined throughout the life of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.2 Safety Responsibilities
Section: 6.1.2 Lines of Authority and Responsibility

Regulatory Basis

DOE/RL-96-0006	*4.1.2.2*	*Safety Responsibility-Safety Assignments*
DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*

7.1 Management and Organization/Staffing

Safety Criterion: 7.1 - 1

Safety management shall oversee the implementation of the risk management program elements. A qualified person shall be assigned the overall responsibility for the development, implementation, and integration of the risk management program elements. If responsibility for implementing individual requirements of the risk management program is assigned to other persons, the names or positions of these people shall be documented and the lines of authority defined through an organization chart or similar document.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 6.1 Integration into Work Planning and Performance

Regulatory Basis

Safety Criterion: 7.1 - 2

When selecting a subcontractor, information regarding the subcontract employer's safety performance and programs shall be obtained and evaluated. Subcontract employees shall be informed of the known potential fire, explosion, or toxic release hazards related to the subcontractor's work and the process. The applicable provisions of the emergency plan shall be explained to the subcontractors. Safe work practices to control the entrance, presence, and exit of subcontract employers and employees in radioactive or hazardous process areas shall be developed and implemented. The performance of subcontract employers with regard to safety shall be periodically evaluated and a subcontract employee injury and illness log related to the subcontractor's work in process areas shall be maintained.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.2 Control of Subcontractors

Regulatory Basis

DOE/RL-96-0006 5.2.5 Subcontractors

Safety Criterion: 7.1 - 3

A framework shall be established for safety review organizations that are responsible for assuring the safety of the facility. The separation between the responsibilities of the safety review organizations and those of the other organizations shall remain clear so that the safety review organizations retain their independence as safety authorities. Internal safety oversight should be conducted by qualified personnel to ensure that the safety standards are consistently met.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.13 Procedures
- Section: 3.16 Internal Safety Oversight
- Chapter: 10.0 Assessments

Regulatory Basis

DOE/RL-96-0006	*4.1.4.1*	*Safety/Quality Culture-Safety/Quality Culture*
DOE/RL-96-0006	*4.3.1.5*	*Conduct of Operations-Internal Surveillance and Audits*
DOE/RL-96-0006	*4.4.1*	*Safety Review Organization*
DOE/RL-96-0006	*4.4.2*	*Qualified Personnel*
DOE/RL-96-0006	*5.1.3*	*Process Safety Responsibility*

Safety Criterion: 7.1 - 4

Commitments from outside organizations to provide data and services required to satisfy safety obligations shall be made prior to the need for the information or services.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.18 Emergency Planning
- Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006	*4.1.2.3*	*Safety Responsibility-Site and Technical Support*

7.2 Training and Procedures

Safety Criterion: 7.2 - 1

Programs providing for continual training and qualification for operations, maintenance, and technical support personnel, to enable them to perform their duties safely and efficiently, shall be developed and implemented utilizing a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.12 Training
Section: 3.15 Training and Qualification
Section: 4.2.2 Training and Procedures

Regulatory Basis

DOE/RL-96-0006	*4.3.1.7*	*Conduct of Operations-Access to Technical Safety Support*
DOE/RL-96-0006	*4.3.4.2*	*Training and Qualifications-Training Programs*

Safety Criterion: 7.2 - 2

A training program must be established, implemented, and maintained for individuals relied upon to operate, maintain, or modify the facility in a safe manner. The training program shall be based on a systems approach to training that includes the following:

(a) Systematic analysis of the jobs to be performed

(b) Learning objectives derived from the analysis which describe desired performance after training

(c) Training design and implementation based on the learning objectives

(d) Evaluation of trainee mastery of the objectives during training

(e) Evaluation and revision of the training based on the performance of trained personnel in the job setting

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification

Safety Criterion: 7.2 - 3

Each employee involved in operating a process shall be trained in an overview of the process and in the operating procedures/instructions. The training shall include emphasis on the specific safety and health hazards, operating limits, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.

Refresher training shall be provided at least every three years, and more often if necessary, to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures/instructions of the process and is proficient in the procedures to follow if conditions exceed the design basis of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.3 Development of the Operator Training Program

Regulatory Basis

DOE/RL-96-0006 4.3.4.1 Training and Qualifications-Personnel Training
DOE/RL-96-0006 4.3.4.3 Training and Qualifications-Conditions Beyond Design Basis
DOE/RL-96-0006 5.2.4 Training
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

Safety Criterion: 7.2 - 4

Up-to-date records of training status shall be maintained which contain the names of the trained employees, the types of training, the dates of training, and the means used to verify that the employees understood the training.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

Safety Criterion: 7.2 - 5

Written procedures/instructions that provide clear direction for safely conducting activities involving radioactive or hazardous materials shall be developed and implemented for each phase of the facility life. The procedures/instructions shall address at least the following elements:

(1) Steps for each operating phase:
   - (a) Initial startup
   - (b) Normal operations
   - (c) Temporary operations
   - (d) Emergency shutdown including the conditions under which emergency shutdown is required, and the assignment of shutdown responsibility to qualified operators to ensure that emergency shutdown is executed in a safe and timely manner
   - (e) Emergency operations
   - (f) Normal shutdown
   - (g) Startup following a turnaround, or after an emergency shutdown

(2) Operating limits:
   - (a) Consequences of deviation
   - (b) Steps required to correct or avoid deviation

(3) Safety and health considerations:
   - (a) Properties of, and hazards presented by, the chemicals used in the process
   - (b) Precautions necessary to prevent exposure, including engineering controls, administrative controls, and personal protective equipment
   - (c) Control measures to be taken if physical contact or airborne exposure occurs
   - (d) Quality control for raw materials and control of hazardous chemical inventory levels
   - (e) Any special or unique hazards

(4) Safety systems and their functions

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.1 Procedure Development

Regulatory Basis

DOE/RL-96-0006	*4.3.2.2*	*Radiation Protection-Procedures and Monitoring*
DOE/RL-96-0006	*5.2.3*	*Operating Procedures*

Safety Criterion: 7.2 - 6

Operating procedures shall be readily accessible to employees who work in or maintain a process with radioactive or hazardous materials.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.1 Procedure Development

Regulatory Basis

Safety Criterion: 7.2 - 7

Operating procedures shall be reviewed as often as necessary to assure that they reflect current operating practice, including changes that result from changes in process chemicals, technology, and equipment, and changes to facilities. These procedures shall be certified annually that they are current and accurate.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.3 Configuration Management
Section: 5.6.1 Procedure Development

Regulatory Basis

Safety Criterion: 7.2 - 8

Safe work practices providing for the control of hazards during operations such as lockout/tagout; confined space entry; opening process equipment or piping; and control over entrance into a facility by maintenance, subcontractor, laboratory, or other support personnel shall be developed. These safe work practices shall apply to employees and subcontractor employees.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.4 Safety/Quality Culture
Section: 5.2 Control of Subcontractors
Section: 5.6.6 Hot Work Operations

Regulatory Basis

7.3 Quality Assurance Program

Safety Criterion: 7.3 - 1

The following quality assurance elements shall be applied using a graded approach:

(1) Quality Assurance Program
(2) Personnel Training and Qualification
(3) Quality Improvement
(4) Documents and Records
(5) Work Processes
(6) Design
(7) Procurement
(8) Inspection and Acceptance Testing
(9) Management Assessment
(10) Independent Assessment.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.11 Quality Levels

Regulatory Basis

10 CFR 830.120 Quality assurance requirements Location: (b)(1)
DOE/RL-96-0006 4.1.6.1 Quality Assurance-Quality Assurance Application
DOE/RL-96-0006 4.1.6.2 Quality Assurance-Established Techniques and Procedures

Safety Criterion: 7.3 - 2

A written Quality Assurance Program (QAP) shall be developed, implemented, and maintained. The QAP shall describe the organizational structure, functional responsibilities, levels of authority, and interfaces for those managing, performing, and assessing the work. The QAP shall describe management processes, including planning, scheduling, and resource considerations.

Implementing Codes and Standards

ASME NQA-1-1989
Section 2, "Quality Assurance Program" (including associated supplements)

Regulatory Basis

10 CFR 830.120 Quality assurance requirements Location: (a)(1)
10 CFR 830.120 Quality assurance requirements Location: (c)(1)(i)
DOE/RL-96-0006 4.1.1.6 Defense in Depth-Human Aspects
DOE/RL-96-0006 4.1.4.1 Safety/Quality Culture-Safety/Quality Culture
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (6)

Safety Criterion: 7.3 - 3

Personnel shall be trained and qualified to ensure they are capable of performing their assigned work. Personnel shall be provided continuing training to ensure that job proficiency is maintained.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.15 Training and Qualification

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(1)(ii)*

Safety Criterion: 7.3 - 4

Documents shall be prepared, reviewed, approved, issued, used, and revised to prescribe processes, specify requirements, or establish design. Records shall be specified, prepared, reviewed, approved, and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
Section 3S-1, 7, "Documentation and Records" (including associated supplements)
Section 3S-1, 17, "Quality Assurance Records" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(1)(iv)*

Safety Criterion: 7.3 - 5

Work shall be performed to established technical standards and administrative controls using approved instructions, procedures, or other appropriate means. Items shall be identified and controlled to ensure their proper use. Items shall be maintained to prevent their damage, loss, or deterioration. Equipment used for process monitoring or data collection shall be calibrated and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
Section 3, "Design Control" (including associated supplements)
Section 5, "Instructions, Procedures, and Drawings" (including associated supplements)
Section 8, "Identification and Control of Items" (including associated supplements)
Section 9, "Control of Processes" (including associated supplements)
Section 12, "Control of Measuring and Test Equipment" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(2)(i)*
DOE/RL-96-0006 *4.1.6.3 Quality Assurance-Established Techniques and Procedures*

Safety Criterion: 7.3 - 6

Processes to detect and prevent quality problems shall be established and implemented. Items, services, and processes that do not meet established requirements shall be identified, controlled, and corrected. Correction shall include identifying the causes of problems and preventing recurrence. Item characteristics, process implementation, and other quality-related information shall be reviewed and the data analyzed to identify items, services, and processes needing improvement.

Implementing Codes and Standards

ASME NQA-1-1989
- Section 15, "Control of Nonconforming Items" (including associated supplements)
- Section 16, "Corrective Action" (including associated supplements)

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(1)(iii)*
DOE/RL-96-0006	*4.1.4.1 Safety/Quality Culture-Safety/Quality Culture*	

Safety Criterion: 7.3 - 7

Inspection and testing of specified items, services, and processes shall be conducted using established acceptance and performance criteria. Equipment used for inspections and tests shall be calibrated and maintained.

Implementing Codes and Standards

ASME NQA-1-1989
- Section 10, "Inspections" (including associated supplements)
- Section 11, "Test Control" (including associated supplements)
- Section 12, "Control of Measuring and Test Equipment" (including associated supplements)

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(2)(iv)*

Safety Criterion: 7.3 - 8

Managers shall assess their management processes. Problems that hinder the organization from achieving its objectives shall be identified and corrected.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Chapter: 10.0 Assessments

Regulatory Basis

10 CFR 830.120	*Quality assurance requirements*	*Location: (c)(3)(i)*

Safety Criterion: 7.3 - 9

Independent assessment shall be planned and conducted to measure item and service quality, to measure the adequacy of work performance, and to promote improvement. The group performing independent assessments shall have sufficient authority and freedom from the line to carry out its responsibilities. Persons conducting independent assessments shall be technically qualified and knowledgeable in the areas assessed.

Implementing Codes and Standards

ASME NQA-1-1989
Section 18, "Audits" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(3)(ii)*

Safety Criterion: 7.3 - 10

Compliance audits shall be performed at least every three years to verify that the procedures and practices developed to ensure nuclear and process safety are adequate and are being followed. The compliance audit shall be conducted by at least one person knowledgeable in the process. A report of the findings of the audit shall be developed. An appropriate response shall be determined and documented for each of the findings of the compliance audit, and it shall be documented when deficiencies have been corrected. Employers shall retain the two most recent compliance audit reports.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.4 Compliance Audits
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 *5.2.12 Compliance Audits*

Safety Criterion: 7.3 - 11

Procured items and services shall meet established requirements and perform as specified. Prospective suppliers shall be evaluated and selected on the basis of specified criteria. Processes to ensure that approved suppliers continue to provide acceptable items and services shall be established and implemented.

Implementing Codes and Standards

ASME NQA-1-1989
Section 7, "Control of Purchased Items and Services" (including associated supplements)

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (c)(2)(iii)*

Safety Criterion: 7.3 - 12

Changes made to the Quality Assurance Program (QAP) shall be submitted annually to the regulator for review. The submittal shall identify the changes, the pages affected, the reason for the changes, and the basis for concluding that the revised QAP continues to satisfy the requirements of this section.

Regulatory Basis

10 CFR 830.120 *Quality assurance requirements* *Location: (b)(3)*

7.4 Unreviewed Safety Questions

Safety Criterion: 7.4 - 1

A safety evaluation shall be performed to determine whether a situation involves an unreviewed safety question (USQ) for:

(1) Temporary or permanent changes in the facility as described in the existing authorization basis

(2) Temporary or permanent changes in the procedures as derived from existing authorization basis

(3) Tests or experiments not described in the existing authorization basis

A situation involves a USQ if:

1) the probability of occurrence or the radiological or chemical consequences of an accident or malfunction of equipment Important to Safety, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility analysis, may be increased

2) a possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis, may be created

3) any margin of safety is reduced

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*
DOE/RL-96-0006	*5.2.9*	*Management of Change*

Safety Criterion: 7.4 - 2

Regulatory approval shall be obtained for situations determined to involve an unreviewed safety question or a change in a technical safety requirement, prior to initiating the activity, if the initiation of the activity would itself involve a USQ, or implementing the proposed change.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*

Safety Criterion: 7.4 - 3

Procedures shall be developed and implemented to govern the need for, and the performance of, safety evaluations.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Safety Criterion: 7.4 - 4

When information is identified that indicates a potential inadequacy of previous analyses as defined in the approved Safety Analysis Report (SAR) or that indicates a possible reduction in safety margins as defined in the technical safety requirements, the following actions shall occur:

(1) Notify the regulator of the situation upon discovery of the information

(2) Perform a safety evaluation

(3) Take action as appropriate to place or maintain the facility in a safe condition until the safety evaluation is completed

(4) Submit the completed safety evaluation prior to removing any operational restrictions initiated

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations

Safety Criterion: 7.4 - 5

For all safety evaluations required under this section, the following actions shall occur:

(1) Document the basis for the USQ(s) determination.

(2) Incorporate in the existing SAR and technical safety requirements for the facility any changes that are needed as a result of the safety evaluation or any action taken pursuant to this section.

(3) Submit to DOE, on a schedule corresponding to the updates of the SAR for the facility, a report summarizing all situations for which a safety evaluation was required by this section and indicating all “changes” considered in a safety evaluation and implemented 3 months or more before the submittal date of the safety analysis report.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation
Section: 3.16.4 Unreviewed Safety Questions

7.5 Conduct of Operations

Safety Criterion: 7.5 - 1

A program for conduct of operations at the facility shall be established and implemented using a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations

Safety Criterion: 7.5 - 2

The conduct of operations program shall address:

(1) Operations organization and administration
(2) Shift routines and operating practices
(3) Control area activities
(4) Communications
(5) Control of on-shift training
(6) Investigation of abnormal events
(7) Notifications
(8) Control of equipment and system status
(9) Lockout and tagout
(10) Independent verification
(11) Logkeeping
(12) Operations turnover
(13) Operations aspects of facility chemistry and unique processes
(14) Required reading
(15) Timely orders to operators
(16) Operations procedures
(17) Operator aid postings
(18) Equipment and piping labeling
(19) Emergency operating procedures for dealing with responses to accident conditions.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations

Regulatory Basis

DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*
DOE/RL-96-0006	*4.3.1.3*	*Conduct of Operations-Emergency Operating Procedures*
DOE/RL-96-0006	*4.3.1.4*	*Conduct of Operations-Readiness*

7.6 Maintenance

Safety Criterion: 7.6 - 1

A maintenance program for the facility shall be developed and implemented using a tailored approach.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 4.2.1 Engineered Features

Safety Criterion: 7.6 - 2

The maintenance program shall contain provisions sufficient to preserve, predict, and restore the availability, operability, and reliability of structures, systems, and components designated as Important to Safety.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI)

Regulatory Basis

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance

Safety Criterion: 7.6 - 3

The maintenance program for Important to Safety Structures, systems and components shall clearly define:

(1) The Important to Safety structures, systems, and components that comprise the facility

(2) The requirements of the maintenance program that are derived from the program elements listed in Safety Criterion 7.6-4

(3) The management systems used for those activities, including the means for monitoring and measuring the effectiveness of the program and the management of maintenance backlog

(4) The assignment of responsibilities and authority for all levels of the maintenance organization

(5) Mechanisms to feedback such relevant information as trend analysis and instrumentation performance/reliability data in order to identify necessary program modifications

(6) Provisions for identifying and evaluating possible component, system design, occupational safety and health, or other relevant problems and implementation of a self-assessment program

(7) Performance indicators and criteria to be utilized to measure equipment, systems, and personnel effectiveness in maintenance activities

(8) Interfaces between maintenance and other organizations (e.g., involving operations, engineering, quality, and safety)

(9) Quantitative reliability target values for systems and components to start or run, when such values are credited in safety analysis

(10) Appropriate authorization is received before modification starts on a safety instrumented system

(11) Assessment of impact of the modification on the functionality of the safety instrumented system is performed, to ensure functionality is not impaired

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
- Section: 1.3.10 Classification of Structures, Systems, and Components
- Section: 3.2 Safety Responsibilities
- Section: 3.4 Safety/Quality Culture
- Section: 3.13 Reliability, Availability, Maintainability, and Inspectability (RAMI)
- Section: 3.16.3 Incident Investigations
- Section: 3.16.5 Performance Monitoring
- Section: 3.16.6 Performance Indicators
- Section: 3.16.8 Feedback and Trending
- Chapter: 10.0 Assessments

24590-WTP-SRD-ESH-01-001-02, Attachment A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 4.2.7.1 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Reliability

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance-Operational Testing, Inspection, and Maintenance

Safety Criterion: 7.6 - 4

The maintenance program shall address each of the following elements:

(1) Organization and administration
(2) Maintenance training and qualification
(3) Maintenance facilities, equipment, and tools
(4) Types of maintenance
(5) Maintenance procedures and other work-related documents
(6) Planning, scheduling, and coordinating maintenance activities
(7) Control of maintenance activities
(8) Post-maintenance testing
(9) Procurement of parts, materials, and services
(10) Material receipt, inspection, handling, storage, retrieving, and issuance
(11) Control and calibration of measuring and test equipment
(12) Maintenance tools and equipment control
(13) Documented facility condition inspections to identify and address aging effects
(14) Management involvement with facility operations
(15) Maintenance history and trending
(16) Analysis of maintenance-related problems
(17) Modification work.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.11 Quality Levels
Section: 4.2.2 Training and Procedures
Section: 5.3 Configuration Management
Section: 5.4 Compliance Audits
Section: 5.6.5 Mechanical Integrity
Chapter: 11.0 Organization Roles, Responsibilities, and Authorities

Regulatory Basis

DOE/RL-96-0006 4.3.5.1 Operational Testing, Inspection, and Maintenance
DOE/RL-96-0006 5.2.7 Mechanical Integrity
WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

7.7 Reporting and Incident Investigation

Safety Criterion: 7.7 - 1

Each incident which resulted in, or could reasonably have resulted in a major accident shall be investigated. An incident investigation shall be initiated as promptly as possible, but not later than 48 hours following the incident.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations
Section: 5.6.7 Investigations of Incidents

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 2

An incident investigation team shall be established and consist of at least one person knowledgeable in the process involved, including a subcontract employee if the incident involved work of the subcontractor, and other persons with appropriate knowledge and experience to thoroughly investigate and analyze the incident. A report shall be prepared at the conclusion of the investigation which includes at a minimum:

(1) Date of incident

(2) Date investigation began

(3) A description of the incident

(4) The factors that contributed to the incident

(5) Any recommendations resulting from the investigation

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations
Section: 5.6.7 Investigations of Incidents
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 3

A system shall be established to promptly address and resolve the incident report findings and recommendations. Resolutions and corrective actions shall be documented. The report shall be submitted to the regulator for evaluation and in support of regulatory oversight. The report shall be reviewed with all affected personnel whose job tasks are relevant to the incident findings including subcontract employees where applicable. Incident investigation reports shall be retained for five years.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.7 Investigations of Incidents

Regulatory Basis

DOE/RL-96-0006 5.2.10 Incident Investigation

Safety Criterion: 7.7 - 4

The Facility Manager shall categorize reportable incidents as soon as reasonably possible and in all cases within 2 hours of identification of the event or condition. If categorization is not clear, the occurrence shall be conservatively categorized at the higher level being considered. The occurrence categorization shall be elevated, maintained, or lowered, as appropriate, as further information is obtained.

Reportable occurrences shall be categorized in accordance with the following guidance:

"Emergencies" are the most serious reportable occurrences and they require an increased alert status for on-site personnel and, in specified cases, for off-site authorities. Emergencies require a time-urgent notification as part of the facility's comprehensive emergency management program.

"Unusual Occurrences" are the category of non-emergency reportable occurrences that exceed the off-normal occurrence threshold and have significant impact or potential for impact on safety, the environment, health, safeguards and security, or operations.

"Off-Normal Occurrences" are the category of abnormal or unplanned reportable occurrences that adversely affect, potentially affect, or are indicative of degradation in the level of safety, safeguards and security, environmental or health protection, performance or operation of the facility.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.6.7 Investigations of Incidents

Safety Criterion: 7.7 - 5

The Facility Manager shall orally notify the regulator of Emergencies within 15 minutes. In addition, the Facility Manager shall orally notify the regulator of Unusual Occurrences, as soon as practical, but in all cases within 2 hours of categorization. The Facility Manager shall contact the regulator via the Headquarters Emergency Operations Center.

Follow-up Notification. The Facility Manager shall provide follow-up oral notification to the regulator via the Headquarters Emergency Operations Center within two hours of identification of further degradation in the level of safety of the facility or other worsening conditions. A change in a reporting level to an Emergency level is to be orally reported within 15 minutes of the recategorization.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations

Safety Criterion: 7.7 - 6

The Facility Manager shall provide written notification of all reportable occurrences, including summaries of Emergencies, to the regulator before the close of the next business day from the time of categorization of the occurrence (not to exceed 80 hours). An Update Occurrence Report shall be submitted when significant new information (including any changes in categorization) is available.

Completion of the Final Occurrence Report is required when the analysis of the occurrence has been completed, root cause and contributing cause(s) finalized, corrective action(s) determined and scheduled, and lessons learned identified. The Final Occurrence Report shall be submitted to the regulator within 45 days of categorization of the occurrence.

The Occurrence Report shall contain, at a minimum, the following information about each reportable occurrence at the facility:

(1) An alphanumeric occurrence report number identifying the regulatory field office, the contractor, the facility, the year of the occurrence, and the sequential number of the occurrence

(2) The number of occurrences in the report

(3) Category of the occurrence

(4) Regulatory program office responsible for the facility involved

(5) All systems, equipment, structural items, administrative controls, or procedures involved in the occurrence or defect identification, including information related to manufacturers, types, model numbers, size, procedure numbers, and (for defect identification) the number of affected components

(6) Date and time when the occurrence was discovered and categorized

(7) Date and time of notification of regulatory and state and local authorities

(8) A thorough and complete description of what occurred or the defect reported, including a sequence of events and a description of failures (or potential failures and the safety significance with respect to defect identification), so that regulatory and contractor personnel, not familiar with the facility-specific design features or administrative controls employed, can understand the complete occurrence and any substantial safety hazard which could result

(9) Operational status of the facility or equipment at the time of the occurrence, including the status of structures, systems, or components that were inoperable at the start of the event and that contributed to the event

(10) Immediate or remedial actions taken to place the facility, system, or equipment in a safe, stable condition, to return them to service, or to correct or alleviate the anomalous condition, and the results of those actions

(11) Cause of the occurrence, including direct and contributing causes and the root cause

(12) Recommendations about whether further evaluation is required and, if so, before or after returning the facility to operation

(13) Action taken or planned to correct the problem and the identified cause and to prevent recurrence

(14) Impact of the occurrence on the environment, health and safety of workers, the public, and on-site and off-site environs (including quantities and types of radioactive materials released)

(15) Levels and types of contamination, human exposures, and known or projected environmental, safety, and health impacts

(16) Impact of the occurrence on the affected program and/or project

(17) Impact of the occurrence on the adequacy of national codes and standards and regulatory requirements

(18) Lessons learned from the occurrence that could be of importance to other facility operators or that shall be addressed in personnel training or facility procedures

(19) Any previous similar events at the same facility that are known to the Facility Manager

(20) The name and telephone number of a person within the Facility Manager's organization who is knowledgeable about the occurrence

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.17 Incident Investigations

Regulatory Basis

DOE/RL-96-0006 *4.3.1.8 Conduct of Operations-Operational Events*

Safety Criterion: 7.7 - 7

Procedures shall be written and implemented to carry out categorization, notification, and reporting requirements for reportable occurrences.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations
Section: 5.6.7 Investigations of Incidents

Safety Criterion: 7.7 - 8

The services of the Environment Safety & Health (ES&H) reporting system, maintained by the Office of Environment, Safety, and Health, shall be used to meet the documentation and distribution requirements of this section.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.3 Incident Investigations

Safety Criterion: 7.7 - 9

The RPP-WTP contractor shall ensure that subcontractors and suppliers report defective items, materials, and services and shall specify these requirements in applicable procurement documents.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 5.2 Control of Subcontractors

7.8 Emergency Preparedness

Safety Criterion: 7.8 - 1

An emergency response program shall be developed, documented, and implemented for the purpose of protecting public health and the environment. The program shall include the following elements:

(1) An emergency response plan.

(2) Emergency Planning Implementing Procedures to ensure the timely and effective implementation of the provisions of the emergency plan.

(3) A facility emergency response organization, with clearly defined roles, responsibilities and authorities.

(4) A training program that provides initial and annual refresher training for facility response personnel, general employees, and response personnel from other agencies.

(5) Program administration to include maintenance of technical support documents, plans, and procedures, the coordination of activities, and maintenance of appropriate auditable records.

(6) Adequate emergency facilities and equipment to support response.

(7) The scope of the program will be designed to be commensurate with the hazards present at the facility and will be determined by performing an assessment of the hazards.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

WAC 246-247 Radiation Protection - Air Emissions Location: Part 075 (12)

Safety Criterion: 7.8 - 2

The Emergency Management Program will be documented in an emergency plan which describes the provisions for responses to Operational Emergencies. The emergency response plan will address the following program elements

(1) The establishment and maintenance of a facility emergency response organization with clearly specified authorities and responsibilities for emergency response and mitigation.

(2) Provisions for interfaces and coordination with Hanford Site and offsite agencies in the areas of planning, preparedness, response, and recovery.

(3) A description of the hazards and potential consequences resulting from analyzed accidents.

(4) Identify and describe the capabilities for the detection of emergency events, the methodology for determining event severity and the basis for declaring an emergency.

(5) The methods to be used to provide notification of an emergency event to Hanford Site organizations, offsite response agencies, and Federal, state and local regulatory agencies.

(6) Provisions for assessing the consequences resulting from the release of hazardous materials.

(7) A description of protective actions for responders, workers, and the public, to include provisions for sheltering, evacuation, and personnel accountability.

(8) Medical support during emergency response, to include provisions for ambulance/hospital services and decontamination of injured personnel.

(9) Methodology for the safe-shut down of the facility, reentry to the facility during or after emergency response and provisions for developing a recovery strategy following an accident.

(10) A public information program designed to provide the public, media and employees with accurate and timely information.

(11) A training program will de designed to ensure that personnel are prepared to respond to, manage, mitigate, and recover from emergencies associated with facility operations.

(12) Provisions for the administration of the program, to include a designated program administrator, program assessment and issue resolution, the development and maintenance of technical support documents, plans, and procedures, the coordination of activities, and maintenance of appropriate auditable records.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006	*4.1.2.3*	*Safety Responsibility-Site and Technical Support*
DOE/RL-96-0006	*5.2.11*	*Emergency Planning and Response*

Safety Criterion: 7.8 - 3

Emergency plans shall be prepared before the startup of the facility, and shall be exercised periodically to ensure that protection measures can be implemented in the event of an accident that results in, or has the potential for, unacceptable releases of radioactive materials within and beyond the facility control perimeter.

A determination shall be made of the size of the geographic area surrounding the facility, known as the Emergency Planning Zone (EPZ), within which special planning and preparedness activities will be performed to reduce the potential health and safety impacts from an event involving hazardous materials. The extent of planning and preparedness necessary shall correspond to the type and scope of hazards present and the potential consequences of events.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.18 Emergency Planning
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.3 Emergency Preparedness-Establishment and Continued Exercise of Emergency Plans*

Safety Criterion: 7.8 - 4

The results of analyses of the facility response to accidents with the potential for releases resulting in doses in excess of Environmental Protection Agency and the State of Washington emergency clean-up standards, beyond the RPP-WTP controlled area boundary shall be used in preparing emergency operating procedures which will contain specific instructions for facility operations personnel on the shutdown of facility processes and the mitigation of accidents for all identified off-normal and emergency conditions.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.2 Emergency Preparedness-Accident Management Strategy*

Safety Criterion: 7.8 - 5

The emergency response plan shall be coordinated with the DOE Hanford Site and local community emergency response plans.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.10 Emergency Preparedness

Regulatory Basis

DOE/RL-96-0006 *4.3.3.1 Emergency Preparedness-Offsite Measures*

8.0 Deactivation and Decommissioning

Safety Criterion: 8.0 - 1

There shall be an approved plan for deactivation of the facility before it is constructed. The objectives of the plan shall be to reduce radiation exposure to Hanford Site personnel and the public both during and following deactivation and decommissioning activities and to minimize the quantity of radioactive waste generated during deactivation, decontamination, and decommissioning. Features and procedures that simplify and facilitate decommissioning shall be identified during the planning and design phase based upon a proposed decommissioning method.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix F, Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning

Regulatory Basis

DOE/RL-96-0006 4.2.3.3 Radiation Protection-Deactivation, Decontamination, and Decommissioning Design
DOE/RL-96-0006 4.3.2.3 Radiation Protection-Final Deactivation Plans and Provisions

Safety Criterion: 8.0 - 2

Facilities shall be designed to simplify decontamination and decommissioning, reduce exposure to site personnel and the public during these activities, and increase the potential for reuse. Features and procedures that simplify and facilitate decontamination, decommissioning, and minimization of contaminated equipment and the generation of radioactive waste during deactivation, decontamination, and decommissioning shall be identified during the planning and design phase based upon a proposed decommissioning method or conversion to other use.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Safety Requirements Document Volume II
Appendix F, Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning
DOE G 441.1-2, Occupational ALARA Program Guide

Regulatory Basis

10 CFR 835 Occupational Radiation Protection Location: 1002
DOE/RL-96-0006 4.2.3.3 Radiation Protection-Deactivation, Decontamination, and Decommissioning Design
DOE/RL-96-0006 4.3.2.3 Radiation Protection-Final Deactivation Plans and Provisions

9.0 Documentation and Submittals

Safety Criterion: 9.0 - 1

An annual report shall be prepared and submitted to the Regulator and appropriate local officials. The annual report shall document:

(1) the quantity of each of the principal radionuclides in excess of background released to unrestricted areas in liquid and gaseous effluents during the previous year of operation.

(2) the calculated annual dose to the maximally exposed members of the public, and (3) the calculated collective dose to members of the public from exposures to RPP-WTP radiation sources.

Reports on dose estimates to the public shall include relevant site-specific information, including the locations of members of the public subject to the greatest potential exposures, the population distribution subject to exposures from RPP-WTP activities, and exposure pathways germane to the site. Values of assumed default or site-specific parameters used in calculations shall be discussed and included with the documentation of the calculations.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 104
40 CFR 61 National Emission Standards for Hazardous Air Pollutants Location: 94

Safety Criterion: 9.0 - 2

The Contractor should request authorization for construction only after being satisfied by appropriate internal assessments that the main safety issues have been satisfactorily resolved and that the remainder are amenable to solution before operations are scheduled to begin.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

DOE/RL-96-0006 4.4.3 Recommendation for Initiation of Construction

Safety Criterion: 9.0 - 3

The results of the pre-startup safety review should be submitted to DOE for evaluation and in support of authorization decisions and regulatory oversight.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 9.2 Scheduling of Events for Regulatory Submittals

Regulatory Basis

DOE/RL-96-0006 5.2.6 Pre-startup Safety Review

Safety Criterion: 9.0 - 4

Material that is part of the authorization basis shall be established, documented, and submitted to the DOE for evaluation and in support of decisions and regulatory oversight. The material shall be maintained current with respect to changes made to the facility design and administrative controls and in the light of significantly new safety information.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1 Content of the Authorization Basis
Section: 3.3.2 Control of the Authorization Basis
Section: 3.3.3 Changes to Safety Documentation

9.1 Safety Analysis Reports

Safety Criterion: 9.1 - 1

Safety analyses shall be performed using a tailored approach to develop and evaluate the adequacy of the authorization basis for the facility. Preliminary and Final Safety Analysis Reports shall be prepared to document the safety analyses.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix A, "Implementing Standard for Safety Standards and Requirements Identification"
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Regulatory Basis

DOE/RL-96-0006	*4.1.3.1*	*Authorization Basis-Authorization Basis*
DOE/RL-96-0006	*4.2.1.3*	*Design-Safety Analysis*

Safety Criterion: 9.1 - 2

A SAR shall contain sections that address the following topics:

(1) Site Description
(2) Facility and Process Description
(3) Integrated Safety Analysis
(4) Nuclear Criticality Safety
(5) Technical Safety Requirements
(6) Radiation Safety
(7) Chemical Safety
(8) Fire Safety
(9) Human Factors
(10) Emergency Preparedness
(11) Management Organization
(12) Conduct of Operations
(13) Procedures
(14) Training and Qualification
(15) Deactivation and Decommissioning
(16) Incident Investigations
(17) Records Management
(18) Audits and Assessments
(19) Quality Assurance
(20) Initial Surveillance and In-Service Testing
(21) Maintenance

The SAR should also contain an Executive Summary that provides an overview of the facility safety basis and presents information sufficient to establish a top-level understanding of the facility, its' operation, and the results of the safety analysis.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Safety Criterion: 9.1 - 3

A Preliminary Safety Analysis Report (PSAR) shall be submitted to the regulator only after all major safety issues have been resolved and other safety issues scheduled for completion. The PSAR shall document the facility design and plans for construction and demonstrate adequate planning for the operational phase.

A Final Safety Analysis Report (FSAR) shall be submitted to the regulator for approval prior to authorization to operate a the facility. The FSAR shall document the completed design and construction and provide details on the plans for operation. The FSAR shall include facility and process drawings and fabrication and construction specifications important to the safety analysis of the facility. The FSAR shall identify significant changes made in the facility design and plans for operation from what was presented in the PSAR.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
Appendix G, "Ad Hoc Implementing Standard for Safety Analysis Reports"

Safety Criterion: 9.1 - 4

The FSAR shall be reviewed annually and updated as necessary to ensure that the information is current, remains applicable, and reflects all changes implemented up to 3 months prior to the filing of the updated FSAR. The regulatory approval of any Unreviewed Safety Questions, and the material submitted to the regulator in support of that approval, shall be considered an addendum to the FSAR until the information is incorporated into the FSAR as part of the next periodic update.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.1 - 5

The SAR shall be maintained as a controlled document.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.1 - 6

All responsibilities concerning the facility as identified in the approved SAR shall be carried out.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.2 Safety Responsibilities

Safety Criterion: 9.1 - 7

The hazard analysis shall be submitted for approval as part of the SAR.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 9.0 Scheduling of Safety-Related Activities

Regulatory Basis

9.2 Technical Safety Requirements

Safety Criterion: 9.2 - 1

Technical safety requirements shall be prepared and submitted for approval, and the facility shall be operated in accordance with the approved technical safety requirements.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations
Section: 3.3.1.4 Technical Safety Requirements (TSR)

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.2 - 2

Technical safety requirements shall be based on the Final Safety Analysis Report and any facility-specific commitments made.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements

Safety Criterion: 9.2 - 3

Technical safety requirements shall consist of the following:

(1) Safety Limits (SLs). This section of the technical safety requirements shall contain the safety limits on the process variables. If an SL for a nuclear facility is exceeded, the nuclear facility shall be immediately placed in the most stable, safe condition attainable, including total shutdown, except where such action might reduce the margin of safety. The safe, stable condition entered as a corrective action shall be maintained until DOE authorizes further operations.

(2) Operating Limits:

(a) Limiting Control Settings (LCSs). This section of the technical safety requirements shall contain the settings for automatic alarms and for the automatic or non-automatic initiation of protective actions related to those variables associated with the function of Safety Design Class structures, systems, or components (SSCs) (if the safety analyses show that they are relied upon to mitigate or prevent an accident). The specific settings chosen must correct a situation automatically or manually such that the related SL is not exceeded. If an automatic alarm or protective device does not function as required during an applicable operating mode, the contractor shall take action as defined in the LCS to maintain the variables within the requirements and to repair the automatic device promptly or to shut down the affected part of the process and, if required, to shut down the facility.

(b) Limiting Conditions for Operation (LCOs). This section of the technical safety requirements shall contain the limits on functional capability or performance level. If a limiting condition for operation is not met, the contractor shall take any remedial actions specified by the technical safety requirements until the condition can be met.

The LCOs will be based upon:

(a) Process variables, design features, and operating restrictions that are the initial conditions for accident analysis.

(b) Structures, systems, and components that must function to prevent or mitigate accidents to achieve compliance to offsite radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2.

(3) Surveillance Requirements (SRs). This section of the technical safety requirements shall contain the surveillance requirements necessary to maintain operation of the facility within the SLs, LCSs, and LCOs. If a required surveillance is not successfully completed or is not performed with its required frequency, the systems or components involved shall be assumed to be inoperable and actions defined by LCSs or LCOs shall be taken until the systems or components can be shown to be operable.

(4) Administrative Controls. This section of the technical safety requirements shall contain the requirements associated with administrative controls, including those for reporting violations of the technical safety requirements. Staffing requirements for facility positions important to safe operation of the facility shall be included in the administrative controls section of the technical safety requirements. Commitments to the safety management programs identified in the SAR as necessary components of the facility safety basis shall be provided in this section.

(5) Use and Application. This section of the technical safety requirements shall contain the basic instructions for applying the safety restrictions contained in the technical safety requirements. Definitions of terms, operating modes, frequency notations, and actions to be taken in the event of violations of OLs or SRs are to be included in this section.

(6) Appendices.

(a) Basis. This appendix shall provide summary statements of the reasons for the OLs and associated SRs. The basis shall show how the numeric value, the condition, or the surveillance fulfills the purpose derived from the safety documentation. The primary purpose for describing the basis of each requirement is to ensure that any future changes to the requirement will not affect its original intent or purpose.

(b) Design Features. This appendix shall describe design features of the facility that, if altered or modified, would have a significant effect on safe operation. If design features are described in a regulator-approved SAR pursuant to this part, this appendix is not required.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)

Regulatory Basis

DOE/RL-96-0006 4.3.1.6 Conduct of Operations-Operations Within the Authorization Basis

Safety Criterion: 9.2 - 4

Technical safety requirements shall be kept current at all times so that they reflect the facility as it exists and as it is analyzed in the SAR.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements

Regulatory Basis

DOE/RL-96-0006 4.1.3.1 Authorization Basis-Authorization Basis

Safety Criterion: 9.2 - 5

All proposed revisions to technical safety requirements, excluding its bases, shall be submitted for regulatory approval prior to implementation of the revision. The submission shall include the basis for the proposed revision.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.3.3 Changes to Safety Documentation

Safety Criterion: 9.2 - 6

Only current approved technical safety requirements shall be used for the operation of the facility. Technical safety requirements shall be maintained as a controlled document with all users designated as authorized users.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.15 Operations
Section: 3.3.1.4 Technical Safety Requirements (TSR)
Section: 4.2.3.4 Technical Safety Requirements and Licensee Controlled Requirements
Chapter: 8.0 Document Control and Maintenance

9.3 Risk Management Plan (this section has been deleted)

Safety Criterion: 9.3 - 1

This safety criterion has been deleted.

All text on this page has been deleted.

Safety Criterion: 9.3 - 2

This safety criterion has been deleted.

Safety Criterion: 9.3 - 3

This safety criterion has been deleted.

Safety Criterion: 9.3 - 4

This safety criterion has been deleted.

Safety Criterion: 9.3 - 5

This safety criterion has been deleted.

Appendix A

Implementing Standard for Safety Standards and Requirements Identification

CONTENTS

1.0 Introduction A-1
2.0 Process Initiation A-1
3.0 Identification of Work A-2
4.0 Hazard Evaluation A-3
4.1 Identification of Hazards A-4
4.2 Identification of Potential Accident/Event Sequences A-4
4.3 Estimation of Consequences A-4
4.3.1 Accident Severity Level Identification A-4
4.3.2 Accident Analysis A-5
4.3.3 Normal Conditions A-6
4.4 Estimation of Accident Frequencies A-7
4.5 Consideration of Common Cause/Common Mode failures A-7
4.6 Definition of Design Basis Events A-8
4.7 Definition of Operating Environment A-8
4.8 Identification of Potential Controls A-8
4.9 Documentation A-9
5.0 Development of Control Strategies A-10
6.0 Classification of Structures, Systems, and Components A-14
7.0 Identification of Standards A-16
8.0 Confirmation of Standards A-18
9.0 Formal Documentation A-18
10.0 Recommendation A-18
11.0 Definitions A-19

1.0 Introduction

This standard implements the process for establishing a set of radiological, nuclear, and process safety requirements and standards as described in DOE/RL-96-0004 and RL/REG-98-17. The Project refers to this process as Integrated Safety Management (ISM).

The activities described below establish radiological, nuclear and process safety standards and requirements for design, construction, and operation of the facility. Establishment of safety standards and requirements is an iterative process that takes place throughout the life of the project. As the design evolves, the process repeatedly evaluates these standards and requirements based on the evolving design.

The Safety Requirements Document (SRD) provides formal documentation of the standards, which are a result of this process. The SRD is updated as required to reflect the results of successive iterations of the standards and requirements identification process (i.e., the ISM process).

2.0 Process Initiation

The RPP-WTP Project Manager shall ensure implementation of the Project Management Plan, thus assuring that adequate resources with appropriate technical background are available and organized to perform subsequent tasks. This activity also assures that the input information required for the safety standards and requirements identification process has been collected and organized. This input information includes the top-level safety standards and principles stipulated by DOE in DOE/RL-96-0006 and the laws and regulations applicable to the RPP-WTP project.

The DOE/RL-96-0004 safety requirements and standards identification Process Manager for the project is the Radiological, Nuclear, and Process Safety Manager.

The Process Manager chairs the DOE/RL-96-0004 safety requirements and standards identification Process Management Team (PMT). The PMT is constituted in accordance with project implementing documents and includes managers from the following project organizations:

- Environmental, Safety, & Health
- Engineering
- Operations

The Process Management Team shall oversee the ISM process and shall provide resources and resolve issues as necessary. The PMT shall set up integrated teams for the conduct of ISM on a plant system basis. Individual PMT members shall provide various subject matter experts to help fulfill the roles required of the Integrated Teams for conduct of the ISM process.

3.0 Identification of Work

The aim of this activity is to describe the work that will be performed so that the hazards inherent in the work can be identified and evaluated. Work activity experts who have extensive knowledge of the overall processing approach and are integrally associated with the facility design shall perform this activity. work activity experts shall be drawn from the following RPP-WTP organizations:

- Engineering staff
- Operations staff

When appropriate, the PMT may also draw work activity experts from the staff of other departments, such as from Construction.

In an overall sense, identification of work involves definition of the project mission and identification of the processes that must be performed to accomplish the mission. It includes selection of optimum functions, processes, and parameters through trade studies and definition of functional requirements. Identification of work for the purpose of design development involves definition of various plant systems, structures, and components. This latter definition is the focus for the Integrated Teams created to conduct ISM on a plant system basis.

The product of this activity includes:

- Process description
- System descriptions
- Descriptions of key structures
- Basis of design documents
- PFDs, MFDs, and P&IDs

The results of the identification of work activity shall be documented in the SRD by inclusion or by reference.

The identification of work activity is an iterative process. Identification of work will be reconsidered in light of design evolution, the outcome of hazard evaluations, and the development of hazard control strategies.

4.0 Hazard Evaluation

The aim of the hazard evaluation activity is to identify and characterize the hazards resulting from the work. The integrated teams shall conduct the hazard evaluation activity on a plant system basis. These teams shall include work activity experts (as defined in Section 3.0), hazard assessment experts, and hazard control experts.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Safety Analysis Manager and of the Regulatory Safety Manager. The process management team shall provide additional technical resources as required to evaluate the hazards.

The hazard evaluation shall address hazards inherent in normal operation as well as potential accidents resulting from abnormal internal and external events.

The hazard evaluation shall comprise the following elements:

- Identification of Hazards
- Identification of Potential Accident/Event Sequences
- Estimation of Accident Consequences
- Estimation of Accident Frequencies
- Consideration of Common Cause and Common Mode Failures
- Definition of Design Basis Events
- Definition of Operating Environment
- Identification of Potential Control Strategies
- Documentation

These elements are discussed below.

4.1 Identification of Hazards

The objective of this element is to systematically identify the hazards associated with the defined work.

The integrated teams shall compile a list of hazardous materials and energy sources associated with the facility processes, design, and operations. This list shall be compiled based on the identified work. This compilation provides information used to identify potential accidents resulting in the uncontrolled release of hazardous material or energy to workers, the public, and the environment. The team may use checklists to guide the compilation process and to assure that all potential hazards from both natural and manmade sources originating from outside and inside the facility are addressed.

4.2 Identification of Potential Accident/Event Sequences

The objective of this element is to perform a structured and systematic examination of the facility and its operations to identify potential accidents (including common mode and common cause failures). The team shall conduct this examination using methodologies and guidelines in AIChE (1992).

4.3 Estimation of Consequences

4.3.1 Accident Severity Level Identification

A severity level, SL, shall be assigned to each postulated radiological accident. The severity level shall reflect the unmitigated consequences of the postulated accident. Unmitigated consequences shall account for the quantity, form and location of the radioactive material available for release, and the energy sources available to interact with the hazardous material. Unmitigated consequences shall not account SSCs that serve to prevent or mitigate the release. Specifically, unmitigated consequences shall be evaluated on the basis of a ground level release. The severity level shall be defined as follows:

SL	Facility Worker Consequence	Collocated Worker Consequence	Public Consequence
SL-1	> 25 rem/event	> 25 rem/event	> 5 rem/event
SL-2	5 - 25 rem/event	5 - 25 rem/event	1 - 5 rem/event
SL-3	1 - 5 rem/event	1 - 5 rem/event	0.1 - 1 rem/event
SL-4	< 1 rem/event	< 1 rem/event	< 0.1 rem/event

These severity levels are related to the radiological and process standards of SRD Chapter 2.0 as follows:

- The unmitigated consequences associated with SL-1 events exceed the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-2 events are below the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-3 events are below the radiological standards for unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-4 events are below the radiological standards for anticipated events (SRD Safety Criterion 2.0-1).

Consequences to the facility worker shall be evaluated at the worst-case occupied location. Consequences to the collocated worker and the public shall be evaluated at the locations specified in Appendix D to the *Safety Requirements Document, Volume II*.

Early in the design, the severity level is estimated based on the experience of the Integrated Teams. As the design progresses, these estimates are confirmed through the formal accident analyses described in Section 4.3.2. These accident analyses do not address all of the potential accidents identified, but they do address bounding examples of each type of accident. The team should use the results of the accident analyses to validate the severity level estimates for potential accidents not addressed in the formal accident analyses.

The potential consequences of releases of hazardous chemicals shall also be assessed. The assessment shall consider both the inherent hazard of the chemical itself, and the potential for the chemical hazard to initiate or exacerbate a radiological hazard.

4.3.2 Accident Analysis

Accident analyses provide confirmation that the design satisfies the radiological and process standards in the SRD. Accident analyses also provide confirmation of the severity levels assigned to potential accidents.

The formal accident analyses shall address design basis external events and natural phenomena as well as postulated internal events.

The postulated internal events shall be grouped by type. Accident types applicable to the RPP-WTP include the following:

- Liquid spills
- Spills of solid materials
- Pressurized releases
- Chemical reactions
- Boiling
- Flammable gas ignition (e.g., hydrogen in air)
- Fires
- Load drops
- Radiation exposure
- Criticality

As a minimum, the accident analysis shall address the most severe credible event of each type.

Initially, the accident analysis shall evaluate the unmitigated consequences of the postulated accidents. As control strategies are developed, the accident analysis shall also evaluate the impact of the SSCs that implement the control strategy on the potential consequences.

The accident analysis shall consider the following factors:

- Inventory of material at risk in the scenario.
- The respirable release fraction for the accident scenario. This is a function of the composition of the material at risk, of the form of the material, and of the interaction between the material at risk and the energy available in the accident scenario.
- The fraction of the airborne material released to potentially occupied locations or the environment.
- Bounding atmospheric dispersion coefficients (if appropriate).
- Radiological composition of the material released.
- External radiation field.
- Exposure times.

The accident analysis shall address the potential consequence to facility workers, collocated workers, and the public.

4.3.3 Normal Conditions

Some hazards inherent in normal operation must be mitigated to comply with the standards for normal operation in SRD Chapter 2.0. Such hazards shall be addressed in accordance with the RPP-WTP Radiation Protection Plan.

4.4 Estimation of Accident Frequencies

There is normally insufficient information early in the design to accurately quantify the frequency of postulated internal events because this frequency depends on the design of the SSCs that implement the control strategy used to manage the hazard. At an early stage, frequency evaluations may be based on the team's experience with similar hazards in similar facilities. The team shall validate these estimates as the design develops.

As the design matures, information on the frequency of hazardous events is gained from the use of hazard evaluation techniques that provide frequency data (i.e., HAZOP, FMEA, Event Trees, and Fault Trees). Evaluations of the frequency of failure in redundant systems or in diverse systems using similar equipment shall consider dependent failures.

The frequencies of design basis external events may be derived from existing analyses (e.g., safety analyses for adjacent facilities), from evaluation of historical data (e.g., transportation data), or from site-specific information (e.g., seismic history).

4.5 Consideration of Common Cause/Common Mode failures

The following are typical common cause events:

- Natural phenomena events
- External man made events
- Loss of electrical power
- Fire
- Internal missiles
- Internal flooding

Common cause events should be treated as discrete events in the hazard analysis. The analyses of common cause events shall focus on identifying provisions to prevent the loss of safety function. The analyses of natural phenomena events shall consider induced effects, such as fire and loss of electrical power.

Common mode failures shall be addressed through dependent failure modeling as required by Section 4.4 above.

4.6 Definition of Design Basis Events

The hazard evaluation shall identify a set of internal design basis events. These events shall be selected to define a set of bounding performance requirements for the SSCs relied upon to control the hazards.

The hazard evaluation shall define a set of external man made design basis events. These events shall be selected based on the results of the hazard analysis to define a set of bounding performance requirements for the SSCs relied upon to mitigate these events.

The integrated teams perform the identification of internal and external design basis events.

Design basis natural phenomena shall be as defined in the SRD Safety Criteria 4.1-3 and 4.1-4.

4.7 Definition of Operating Environment

The hazard evaluation shall define a set of bounding operating conditions in which SSCs relied upon to control hazards must function. Environmental parameters to be addressed include the following:

- Temperature
- Pressure
- Humidity
- Radiation Levels
- Chemical Environment

4.8 Identification of Potential Controls

Based on the experience and judgement of team members, the integrated team shall identify an initial set of potential hazard controls to manage each potential accident. This set of potential hazard controls shall address means of preventing the potential accident and should address means of mitigating the consequences of the accident. The function(s) of each potential hazard control should be clearly described. Potential hazard controls shall be identified to manage accident conditions arising from upsets in the process, conditions arising from external events, and conditions inherent in the normal operation of the process.

4.9 Documentation

The hazard evaluation shall be documented in a hazard analysis report (HAR). The results of the hazard evaluation shall be contained in a hazard database. For each hazard considered, the hazard database shall record the following information produced by the hazard evaluation:

- Hazard identifier
- Hazard description
- Initiators
- Hazard severity level estimate (based on unmitigated consequences)
- Severity level basis
- Assumptions affecting the release (material at risk, energy available, etc)
- Hazard frequency estimate
- Basis for frequency estimate
- Potential controls and functions
- References for the hazard (these would typically be products of the work identification process)

Hazard evaluation documentation shall be included in the SRD by inclusion or by reference. This documentation shall include the following:

- Description of the comprehensive approach to hazard evaluation
- Description of the methodology for identification and quantification of work hazards
- Description of the methodology for identifying potential accident scenarios
- Description of the methodology for consequence assessment
- Clear identification of assumptions (e.g., quantity and form of material at risk, rate of release and relevant process conditions) that may drive or inhibit the potential accident must be clearly identified
- Description of results
- Evidence of appropriate staffing, and adequate technical staffing and structure applied to the hazard evaluation

5.0 Development of Control Strategies

The aim of the development of control strategies activity is to identify a means of controlling each of the hazards identified in the hazard evaluation. The integrated teams of work activity experts, hazard assessment experts, and hazard control experts, as discussed in Sections 3.0 and 4.0, perform this activity.

The PMT members shall provide additional technical resources as required to develop the control strategies.

The integrated teams select preferred control strategies based on the set of potential controls identified by the hazard evaluation team. Selection of the preferred strategy considers the following factors:

- The functions required of the strategy in order to control the hazard
- The degree of defense in depth and reliability provided by the control strategy. The Implementing Standard for Defense in Depth provides guidance in this area.
- Applicable design basis events.
- The operating environment in which the SSCs implementing the control strategy must function.
- Effectiveness and efficiency of the control strategy.
- Conformance with the DOE stipulated top level standards.
- Compliance with applicable laws and regulations.

The control strategy will typically comprise a series of elements including some or all of the following:

- Passive and/or active SSCs that function to prevent the release (that is, SSCs that reduce the probability that a release will occur)
- Passive and/or active SSCs that function to mitigate the release (that is, SSCs that reduce the consequences once a release has occurred)
- Administrative controls (for example, limits on inventory)

Consistent with the defense in depth principle, the control strategy development should emphasize preventive measures. It should also emphasize passive SSCs over active SSCs and retention of released material over dispersion. Ideally, the preferred control strategy should incorporate SSCs that prevent releases and SSCs that mitigate the consequences of a release, should it occur.

Once the preferred control strategy is identified, it shall be evaluated using the techniques described in Section 4.3 through 4.5. In addition, the evaluation of the control strategy shall identify the measures necessary to assure that it performs its functions reliably. Such measures include maintenance requirements, testing intervals and calibration frequency. The results of this evaluation serve to confirm that the control strategy is capable of satisfying SRD Safety Criteria 2.0-1.

If credit is taken for operator action to satisfy the public radiological exposure standards of Safety Criterion 2.0-1, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem TEDE whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy public chemical exposure to the standards of Safety Criterion 2.0-2, provisions for operational access and control are made so that the operator exposure does not exceed the limits specified in Safety Criterion 4.3-7.

Documentation of the hazard control strategy development process shall clearly indicate selection of the control strategies and show the linkage of the control strategies to the respective hazards. The control strategy should be described in terms of the safety functions required (e.g., limit release of radionuclides, etc.) and in terms of a set of engineered features, administrative controls (procedures and training), and management systems selected for implementing the strategy. When the nature of the hazard is such that the appropriate control strategy is self-evident, the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria, and need not provide a discussion of other, nonapplicable control strategies. Similarly, where a proven control strategy that is appropriate to the hazard exists and it is obvious to the team that there are no other alternative control strategies that could be equally attractive, then the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria. Otherwise, the documentation should identify all control strategies considered and provide a defensible rationale for selection of the preferred strategy.

The following information produced by the control strategy definition shall be recorded in the hazard database:

- Preferred control strategy
- Linkage of the control strategy to the respective hazards
- Rationale for preferred control strategy selection
- Defense in depth provided
- Control strategy functions and performance requirements
- Estimate of the unmitigated event frequency
- Estimate of the consequences from the mitigated event
- Estimate of the mitigated event frequency
- Applicable design basis events (e.g., design basis earthquake)

One of the issues in developing a control strategy for a particular hazard is determining the number of layers of prevention and mitigation appropriate for the hazard. The control strategies shall conform to the requirements defined in the Implementing Standard for Defense in Depth. In addition, the following guidance shall be considered in developing control strategies.

The general RPP-WTP design approach is to provide two confinement barriers against the release of hazardous materials. The process vessels and piping form the primary confinement barrier; the process cells and associated ventilation system form the secondary confinement barrier. Releases from the primary confinement are mitigated by the secondary confinement.

The accident severity levels defined in Section 4.3.1 are related to the exposure standards in SRD Safety Criterion 2.0-1. The SRD Safety Criterion 2.0-1 exposure standards are frequency based, so it is possible to establish target frequencies for events with a given severity level. The target frequencies tabulated below are consistent with SRD Safety Criterion 2.0-1.

SL	Event Target Frequency (yr^{-1})
SL-1	$<10^{-6}$
SL-2	$<10^{-4}$
SL-3	$<10^{-2}$
SL-4	$<10^{-1}$

These target frequencies may be used to guide control strategy development as described below.
For SL-1 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.
- Meeting the target frequency will usually require diverse SSCs that act to prevent the release.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the preventive SSCs assure that the frequency of release is less than 10^{-4} per year, but more than 10^{-6} per year. This frequency is not acceptable for events that have SL-1 level consequences, but is acceptable for events that have SL-2 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-2 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-1 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.
- SSCs in control strategies for SL-1 events shall satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-2 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the only viable preventive SSCs assure that the frequency of release is less than 10^{-2} per year, but more than 10^{-4} per year. This frequency is not acceptable for events that have SL-2 level consequences, but is acceptable for events that have SL-3 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-3 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-2 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.
- SSCs in control strategies for SL-2 events should satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-3 and SL-4 events:

- The mitigation provided by the secondary confinement would be adequate to satisfy SRD Safety Criterion 2.0-1. It would also be adequate to satisfy SRD Safety Criteria 1.0-3 through 1.0-5. However, preventive features should be considered consistent with the defense in depth principle.
- A single preventive SSC may satisfy the frequency goal for SL-3 and SL-4 events.
- SSCs in control strategies for SL-3 and SL-4 events need not satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

Notwithstanding the foregoing guidance on control strategy selection, administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control.

6.0 Classification of Structures, Systems, and Components

The design classification process used on the RPP-WTP Project provides a consistent, project-wide approach for the classification of the RPP-WTP SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs can be revised as necessary.

The RPP-WTP project has established a design classification system to provide assurance to DOE that the defined safety functions of SSCs will perform as intended.

SSCs defined as Important-to-Safety for the RPP-WTP include the following:

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs are designated as Safety Design Class, as defined by SRD Safety Criterion 1.0-8.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs are designated as Safety Design Significant, as defined by SRD Safety Criterion 1.0-8.

   The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

   Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded or prevent a criticality. However, additional items may also be designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis.

   Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

When an SSC is designated as Safety Design Class it has the following attributes:

1) Quality Level 1 (QL-1) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
2) For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. If the hazard analysis shows that these requirements are necessary, this requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.
3) The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-3.
4) General design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Class SSCs.
5) Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0.
6) Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.
7) Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements.

When an SSC is classified as Safety Design Significant it is has the following attributes.

1) Quality Level 2 (QL-2) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-4.
3) General and specific design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Significant SSCs.
4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

7.0 Identification of Standards

Identification of standards is an iterative activity. Initially, the set of standards and requirements is derived from a general understanding of the hazards inherent in the work. As the design evolves, the hazard evaluation and the development of the control strategies justify tailoring the set of standards to better fit the hazards.

The identification of engineering/design, manufacture/fabrication, and construction standards is performed by an integrated team including work activity experts, hazard assessment experts, hazard control experts, as discussed in Sections 3.0 and 4.0, and standards experts. Identification of other standards (e.g., quality assurance, conduct of operations, etc.) will be performed by specially constituted teams formed by the PMT. The aim of this activity is to identify a tailored set of standards and requirements that will assure adequate safety when implemented.

The process management team shall provide additional technical resources as required to identify the standards.

Standards experts shall be drawn from the following RPP-WTP organizations:

- Staff of the Engineering Manager
- Technical staff of the ES&H Manager

The standards identified are evaluated and tailored for each control strategy based on compliance with applicable laws and regulations and conformance with the DOE-stipulated top level standards, plus the output of the preceding hazard evaluation and control strategy development steps. Typical considerations include the following:

- The severity level of the hazard
- The number of independent SSCs that comprise the control strategy
- The control strategy functions - recognizing that a specific control strategy may have multiple functions and serve to control multiple hazards
- The service environment
- The applicable design basis events
- The target reliability for the control strategy

The target frequencies described in Section 4 provide a basis for establishing target reliabilities for the SSCs that comprise the control strategy. The combined reliability of the preventive SSCs and the SSCs that provide mitigation must be consistent with the target frequency for the unmitigated event. The reliability of the preventive SSCs should be consistent with the release frequency used to determine the degree of mitigation provided.

Documentation of the standards and requirements identification process provides justification of the set selected and links each control strategy to its associated set of standards. The information generated during standards selection is retained in database form for each control strategy:

- Control strategy
- Service environment
- Applicable design basis events
- Applicable standards
- Performance requirements
- Testing/calibration requirements
- In-service inspection requirements
- Maintenance requirements
- Quality level
- Standards justification

This information is structured so it can be linked to the control strategies in the hazard schedule. This provides a link from the hazards through the control strategies to the standards. Not all of this information will be available early in the design. For example, it will not be possible to define maintenance and testing requirements until the design is mature.

The standards identified through this activity shall be reflected in the SRD.

As the standards are tailored, discrepancies with the current version of the SRD may arise. Such discrepancies shall be recorded. Formal changes to the SRD require approval from DOE.

8.0 Confirmation of Standards

Based on the recommendation of the PMT, the RPP-WTP Project Safety Committee (PSC) Chair requests the PSC to confirm the selected set of standards. The PSC defines a review approach, carries out the review, and documents the findings of the review. Comments by the PSC shall receive formal disposition by the Process Management Team.

9.0 Formal Documentation

Following confirmation by the PSC, the results of the standards selection process shall be documented in the Safety Requirements Document (SRD). The SRD shall incorporate documentation supporting these results by reference. The SRD shall identify and justify the set of requirements and standards selected to provide adequate protection of workers, the public, and the environment.

10.0 Recommendation

The recommended set of standards shall be certified in accordance with project implementing documents. When properly implemented, the set of standards:

1) Provides adequate safety
2) Complies with applicable laws and regulations
3) Conforms with the Top-Level Safety Standards and Principles

11.0 Definitions

Credible event: Any event with a frequency greater than 10^{-6} per year, including allowance for uncertainties.

Important to Safety: Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related, or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related, may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Mitigated event: As used in this standard, a mitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Mitigation of the consequences of the release as provided by the control strategy

Mitigated event frequency: The mitigated event frequency is the corresponding release frequency times the probability that the elements of the control strategy that mitigate the release will function given the release.

Release frequency: The release frequency is the product of the frequency of the initiating event times the probability that all elements of the control strategy that would prevent the release fail, given the initiating event.

Reliability: The probability that an SSC will perform its safety function when required.

Unmitigated event: As used in this standard, an unmitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Failure of all elements of the control strategy that would mitigate the consequences of the release

Unmitigated event frequency: The frequency of an unmitigated event is the corresponding release frequency times the probability that all elements of the control strategy that would mitigate the release fail, given the release.

Appendix B

Implementing Standard for Defense in Depth

CONTENTS

1.0 Introduction B-1
2.0 Standards for the Implementation of Defense in Depth Sub-Principles B-1
2.1 Defense in Depth B-2
2.1.1 Implementing Standards B-2
2.1.2 Discussion B-2
2.2 Prevention B-4
2.2.1 Implementing Standards B-4
2.2.2 Discussion B-4
2.3 Control B-5
2.3.1 Implementing Standards B-5
2.3.2 Discussion B-6
2.4 Mitigation B-7
2.4.1 Implementing Standards B-7
2.4.2 Discussion B-7
2.5 Automatic Systems B-8
2.5.1 Implementing Standards B-8
2.5.2 Discussion B-8
2.6 Human Aspects B-9
2.6.1 Implementing Standards B-9
2.6.2 Discussion B-9
3.0 Determination of SSCs for the Implementation of Defense in Depth B-12
4.0 Definitions B-15
5.0 References B-20
6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth B-21
6.1 DOE O 420.1, Facility Safety (Ref. 5.2) B-21
6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3) B-21
6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7) B-22
6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8) B-22
6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9) B-23
6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11) B-24
6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12) B-25
6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13) B-25

1.0 Introduction

The purpose of this Implementing Standard is to consolidate the standards to be applied in the design, construction, and operation of the RPP-WTP with respect to defense in depth. This Implementing Standard also provides for tailoring of defense in depth as is appropriate to the nature and severity of the hazard and hazardous situations to which it is applied.

Section 2.0 identifies the subordinate standards used in the application of the six defense in depth sub-principles of DOE/RL-96-0006. These subordinate standards are derived, in part, from various available consensus standards. In cases where no relevant consensus standard exists for a given defense in depth sub-principle, this document provides the criteria to be implemented.

Section 3.0 discusses the approach to be used in implementing defense in depth with respect to determining an adequate combination of passive barriers and active SSCs that afford protection against a postulated initiating event.

Terms used in this Implementing Standard are defined in Section 4.0. These definitions are derived from consensus standards, tailored to the work and hazards of the RPP-WTP.

2.0 Standards for the Implementation of Defense in Depth Sub-Principles

The Top Level Principles identify the following sub-principles that must be addressed in order to demonstrate compliance with the principle of defense in depth:

- Defense in depth
- Prevention
- Control
- Mitigation
- Automatic Systems
- Human Aspects

The following subsections contain the standards on application of the six sub-principles of defense in depth from DOE/RL-96-0006 (Ref. 5.4). These consensus standards will be tailored to remove obviously reactor-specific and other non-applicable criteria. In accordance with the DOE/RL-96-0004 process, further tailoring will be performed as the design develops.

The following subsections contain excerpts and extracts from several consensus standards. Where necessary to avoid the implication of misquoting, differences in wording from the cited consensus standards are identified by presenting added words in italics and by inserting double-brackets where words have been removed. Citation of a portion of a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

2.1 Defense in Depth

"To compensate for potential human and mechanical failures, a defense-in-depth strategy should be applied to the facility commensurate with the hazards such that assured safety is vested in multiple, independent safety provisions, not one of which is to be relied upon excessively to protect the public, the workers or the environment. This strategy should be applied to the design and operation of the facility." (DOE/RL-96-0006, Section 4.1.1.1)

2.1.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)
4. IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

2.1.2 Discussion

The RPP-WTP will be designed with the objective of providing multiple *levels* of protection to prevent or mitigate the unintended release of radioactive materials to the environment. Defense in depth will include: siting; minimization of material at risk; the use of conservative design margins and quality assurance; the use of successive physical barriers for protection against the release of radioactivity; the provision of multiple means to control critical safety functions (those basic safety functions needed to control the processes, maintain them in a safe state, and to confine and mitigate radioactivity associated with the potential for accidents with significant [ ] radiological impact *to the public, facility workers or collocated workers*); the use of equipment and administrative controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition; means to monitor accident releases required for emergency responses; and the provision of emergency *preparedness* for minimizing the effects of an accident (Ref. 5.2).

The defense-in-depth concept is integrated into the RPP-WTP design process. The application of the defense-in-depth concept to the facility design helps identify potential safety features to be included in the facility design. Consideration will be given to prevent or mitigate accident consequences from contaminating the environment, even when direct public or worker safety is not an issue.

Defense in depth is a safety design concept or strategy that is applied at the beginning and will be maintained throughout the facility design process. This safety design strategy is based on the premise that no one *level* of protection is completely relied upon to ensure safe operation. This safety strategy provides multiple *levels* of protection to prevent or mitigate an unintended release of radioactive material to the environment.

Conceptually, there are three levels of defense in depth.

1. The first level of defense consists of a well-designed facility with process design to reduce source terms, reliable SSCs that are simple to operate and maintain and resistant to degradation, and personnel well trained in operations and maintenance and committed to a strong safety culture.
2. The second level recognizes that failures of systems and components and human failures cannot be entirely eliminated and that protective features (e.g., engineering design features and administrative controls) are required. These features are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of anticipated, but abnormal events. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.
3. The final level of defense consists of conservatively designed *important to* safety SSCs to prevent or mitigate the consequences of accidents that may be caused by errors, malfunctions, or events that occur both internal and external to the facility (Ref. 5.3).

Implementing Standards for the following elements of defense in depth described in the nonreactor safety Implementation Guide (IG) related to safety design and construction are addressed in the sections of this document that are referenced below.

IG Element	Discussed in Section
Siting	2.2.2
Material at risk	2.2.2
Conservative design	2.2.2
Quality assurance	2.6.2
Physical barriers	2.4.2
Critical safety functions	2.3.2
Equipment and administrative controls	2.3.2 and 2.6.1
Emergency features	2.5.2

When active SSCs are required to achieve defense in depth, RPP-WTP will apply the single failure criterion in accordance with ANSI/ANS-58.9 (Ref. 5.8) for fluid systems and IEEE Std 379 (Ref. 5.9) for electrical and instrumentation and control systems, as discussed below.

The application of the single failure criterion begins with the identification of an initiating event. Initiating events are identified in the normal course of applying integrated safety management in accordance with DOE/RL-96-0004, as described in the RPP-WTP Implementing Standard for Safety Standards and Requirements Identification (i.e., SRD Vol. II, Appendix A). In evaluating the defense in depth of the RPP-WTP, single failures must be postulated in addition to the initiating event (that is the initiating event is not the single failure) (Ref. 5.8). For fluid systems, during the short term, the single failure considered may be limited to an active failure. During the long term, assuming no prior failure during the short term, the limiting single failure considered can be either active or passive. Examples of passive failures are valve packing and pump seal leakage.

Tailoring of the application of the single failure criterion to the work and associated hazards is discussed in Section 3.0.

2.2 Prevention

"Principal emphasis should be placed on the primary means of achieving safety, which is the prevention of accidents, particularly any that could cause an unacceptable release." (DOE/RL-96-0006, Section 4.1.1.2)

2.2.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph

2.2.2 Discussion

The provision of hazard elimination and protection shall be optimized by measures such as the choice of siting, proven conservative design and construction, a robust start-up testing program, operating requirements (i.e., clear definition of normal and abnormal operating conditions and maintenance activities).

Siting. The RPP-WTP site location will reduce the need to provide design measures to alleviate potentially hazardous conditions or to protect surrounding populations (for example, consideration of ground instability, river flooding, and hazards due to nearby industrial installations or activities) (Ref. 5.3).

Material at Risk. The RPP-WTP and its process design and administrative controls will minimize and control inventories of radioactive materials and their forms (Ref. 5.3).

Conservative Design. The RPP-WTP design will include conservative margins that allow flexibility of operations and maximize the time before requiring corrective actions. These margins will also take into consideration the potential degradation of elements and operational errors (Ref. 5.3).

The design shall address all identified hazards and hazardous situations and pursue methods for their prevention. The preferred means of prevention is to eliminate or reduce the severity of the hazard itself. According to the Implementation Guide on nonreactor facility safety, one objective of prevention as an element of defense in depth is to apply facility and process design and administrative controls to minimize and control inventories of radioactive materials and their forms (that is, minimize the material at risk) (Ref. 5.3).

Elimination or reduction of the hazard can be achieved by substituting less hazardous materials in processing, limiting the inventory of the material, etc. The design process must provide evidence through documentation that this option was considered and implemented to the maximum extent practicable. Where the hazard itself cannot be eliminated or reduced, controls shall be provided to reduce the likelihood of the hazard manifesting itself into an accident. The criterion for acceptability is discussed in Section 3.0. Where hazard elimination is not practicable, passive features are to be employed, since they are simple and have a high degree of reliability. Where this is not practicable, active protection will be proposed that has a degree of reliability and confidence commensurate with the potential hazard severity.

To illustrate the differences between hazard elimination and the provision of passive or active protection, consider the need for a cask lift using a crane. Elimination of the hazardous situation (inherent safety) is removal of the potential for raising a cask above its safe drop height by ensuring that the building dimensions physically prevent a lift above that height at all points of travel. If this were not practical, the provision of a physical stop would be passive protection to prevent a lift above the safe drop height. Active protection systems would include limit switches and braking systems. Procedures and operator training would ensure that the crane is handled and operated in a way that maximizes safety (e.g., check security of load, minimum lift height to confirm security, no challenge to engineered systems, and exclusion of personnel from load lifting area).

2.3 Control

"Normal operation, including anticipated operational occurrences, maintenance and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems and components important to safety is small." (DOE/RL-96-0006, Section 4.1.1.3)

2.3.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
4. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)

2.3.2 Discussion

The DOE Implementing Guidance for nonreactor facility safety provides two criteria related to the defense in depth sub-principle of control:

Critical safety functions. Design to provide multiple ways for safety functions to control processes, to maintain processes in a safe state, and to confine radioactivity when accidents could have the potential for significant [ ] radiological impact *to the public, facility workers or collocated workers* (Ref. 5.3).

Equipment and administrative controls. Include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3).

Normal operations, which include anticipated operational occurrences and maintenance and testing activities, shall be controlled so that facility and system parameters remain within their specified operating ranges and that the frequency of demands placed on SSCs for hazard prevention and mitigation is small.

This will be achieved by the choice of design that will:

1. Control key operating parameters such that facility operations remain within the safe operating envelope. Key operating parameters are those that define how the plant will be operated safely.
2. Maintain the safe operating envelope (e.g., a wide variation in operation conditions can be tolerated without entering into a potentially unsafe region).
3. Ensure that any failure mode would not move the facility or process toward a potentially unsafe region (i.e., fail to safe state).
4. Provide instrumentation and control features (e.g. temperature, pressure, radiation monitoring) which will warn of reduced margins of safety and, where appropriate, automatically return the process into the designated safe operating regime.
5. Achieve independence between SSCs credited for control of normal facility operations and those credited for prevention and mitigation of potential hazards.

For example, assume that the normal operating temperature range in an ion exchange column is set at 30 - 50 °C and that column temperatures above 80 °C lead to enhanced resin degradation and a potential explosion hazard. Engineered controls for maintaining that temperature within the normal operating limits (e.g., temperature control system) will be independent of that which would alert the operator and perform a preventative action (e.g., shut down process, increase cooling, etc.) in order that the hazard could not occur.

2.4 Mitigation

"The facility should be designed to retain the radioactive material through a conservatively designed confinement system for the entire range of events considered in the design basis. The confinement system should protect the workplace and the environment." (DOE/RL-96-0006, Section 4.1.1.4)

2.4.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02, see below)

2.4.2 Discussion

The purpose of mitigation is to ensure reduction of consequences from potential hazards and hazardous situations. One method of achieving this element of defense in depth is to ensure that suitable confinement of radioactive and hazardous material is maintained throughout normal operation and credible accident conditions. Confinement will be achieved by physical barriers and by other SSCs that either assure integrity of the physical barriers or minimize the quantity and characteristics of any hazardous material potentially releasable.

DOE Order 420.1, Chg 2, requires:

> "All nuclear facilities with uncontained radioactive materials (as opposed to material contained within drums, grout and vitrified materials) shall have means to confine them. Such confinement will act to minimize the spread of radioactive materials and the release of radioactive materials in facility effluents during normal operations and potential accidents. For a specific nuclear facility, the number and arrangement of confinement barriers and their required characteristics shall be determined on a case-by-case basis. Factors that shall be considered in confinement system design shall include type, quantity, form, and conditions for dispersing the material. Engineering evaluations, trade-offs, and experience shall be used to develop practical designs that achieve confinement system objectives. The adequacy of confinement systems to effectively perform the required functions shall be documented and accepted through the Safety Analysis Report." (Ref. 5.2)

The DOE nonreactor facility safety Implementation Guide defines confinement barriers to include primary confinement and secondary confinement. "Primary confinement provides confinement of hazardous material to the vicinity of its processing -- typically by means of piping, tanks, glove boxes, encapsulating material, etc., along with any offgas systems that control effluent from the primary confinement. As such, primary confinement addresses the preventive sub-principle of defense in depth, as well as mitigation. Secondary confinement consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area." [ ] (Ref. 5.3)

The RPP-WTP will provide physical barriers to confine radioactive material and thereby prevent uncontrolled releases. In general, multiple physical barriers - i.e., primary and secondary confinement - will be provided, especially for the most severe hazards and hazardous situations. Although RPP-WTP buildings will afford a tertiary confinement, as defined in the Implementation Guide, the RPP-WTP accident analysis will not take credit for holdup of radioactive materials by the buildings. The provision of multiple physical barriers will be tailored to the work and associated hazards, as discussed in Section 3.0.

The DOE nonreactor facility Implementation Guide (IG) suggests several industry consensus codes and standards for the design and construction of the SSCs comprising confinement, as follows: structures - IG subsection 5.2.1, ventilation systems - subsection 5.2.2.1, and process equipment - subsection 5.2.2.2. The specific standards for SSCs that implement mitigation with respect to SSCs comprising confinement are contained in the following Safety Criteria from the Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02):

- Structures - SC 4.1-2
- Ventilation systems - SC 4.4-6 through 4.4-8
- Process equipment - SC 4.2-1 through 4.2-3

2.5 Automatic Systems

"Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints." (DOE/RL-96-0006, Section 4.1.1.5)

2.5.1 Implementing Standards

1. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
2. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)
3. ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

2.5.2 Discussion

Automatic systems shall be provided to prevent the facility from entering into or remaining within an unsafe regime that may lead to the potential for radioactive or hazardous material release to workers, the public, or the environment, except as discussed below. The definition of the boundaries between safe and unsafe regimes will be determined as a result of detailed facility design, start-up, and testing activities. This will allow the derivation of the predetermined setpoints for safe facility operations. Automatic systems will be part of the overall suite of SSCs provided as part of the hazard control strategy. The determination of the need for automatic systems will be assessed as part of the determination of the overall hazards control strategy.

Means shall be provided to automatically initiate and control all protective actions except as justified below. The design of important to safety systems shall be such that the operator is not required to take any action prior to the time described below following the onset of any event (Based on IEEE Std 603-1991 - Ref. 5.11).

Credit for operator action may be permissible only if safety analysis demonstrates that the total time interval required to perform the operator action exceeds the time at which the limiting design requirement would be reached without operator action, in accordance with the methodology of ANSI/ANS-58.8-1994 (Ref. 5.7).

2.6 Human Aspects

"The human aspects of defense in depth should include a design for human factors, a quality assurance program, administrative controls, internal safety reviews, operating limits (Technical Safety Requirements), worker qualification and training, and the establishment of a safety/quality program." (DOE/RL-96-0006, Section 4.1.1.6)

2.6.1 Implementing Standards

1. IEEE Std 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12).
2. Implementing standards for the quality assurance program, administrative controls, internal safety reviews, operating limits (Technical Safety Requirements), worker qualification and training, and the establishment of a safety/quality program are contained in the Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), as discussed below.

2.6.2 Discussion

<u>Design for Human Factors</u>

The design shall apply human factors engineering (HFE) to address the ergonomic requirements of facility operations and maintenance of the RPP-WTP. The DOE nonreactor Implementation Guide recommends that the following human factor elements be considered: equipment labeling, workplace environment (temperature and humidity, lighting, noise, vibration, and aesthetics), human dimensions, operating panels and controls, component arrangement, warning and annunciator systems, and communication systems (Ref. 5.3).

The RPP-WTP design engineers, in consultation with operators, will apply these HFE elements in the design of important to safety SSCs to ensure that operational preferences are implemented. Human factors engineering specialists will provide support in the application of HFE.

Human factors engineering shall be conducted in accordance with IEEE Std 1023-1988 (Ref. 5.12), as discussed below. Selection of this subordinate standard comports with the nonreactor safety Implementation Guide (Ref. 5.3).

IEEE Std 1023-1988 was developed specifically for nuclear power generating stations. Therefore, this subordinate standard will be tailored to the work and hazards of the RPP-WTP as follows. The formal HFE process described in subsection 6.1.1 of IEEE Std 1023-1988 will be applied to the evaluation of hazards whose consequences fall into the two highest severity levels - SL-1 and SL-2, with the following clarification:

> The project does not plan on constructing a separate plant simulator or physical mockup. The RPP-WTP distributed control system (DCS) - including the main control room panels -- is a programmable computer system. The project envisions having the DCS built, delivered to the site and proof-tested with the aid of the facility operators well in advance of plant startup. Therefore, a dynamic simulation capability for personnel training will be provided for SSCs with significant human interfaces that involve complex and interactive processes (Ref. IEEE Std 1023-1988 §§ 6.1.1.12 and 6.1.1.18).

Although the structured HFE program outlined in subsection 6.1.1 of IEEE Std 1023-1988 will not be implemented for SL-3 and SL-4 events, the general HFE elements will be considered for all ITS SSCs, as committed above.

Similarly, formal consideration of the HFE techniques and methodologies recommended in Section 5 of IEEE Std 1023-1988 will be undertaken for hazards of severity levels SL-1 and SL-2. Certain of these techniques and methodologies may be utilized in the evaluation of SL-3 and SL-4 events in the context of the normal design and hazard assessment and control effort, as part of the integrated safety management process.

Quality Assurance Program

The *Safety Requirements Document Volume II* (24590-WTP-SRD-ESH-01-001-02) Safety Criteria 1.0-10 and Section 7.3 require the RPP-WTP contractor to establish and implement a Quality Assurance Program compliant with 10 CFR 830.120. This program is being implemented in accordance with the *Quality Assurance Manual* (24590-WTP-QAM-QA-01-001).

The *Quality Assurance Manual* (24590-WTP-QAM-QA-01-001) applies specifically to work performed on or for the RPP-WTP. The QAP is in conformance with 10 CFR 830.120 (Ref. 5.1) and with the top-level principles stated in DOE/RL-96-0006 (Ref. 5.4).

Administrative Controls

Administrative controls include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3).

The primary means of implementing defense in depth is through the provision of multiple physical barriers that maintain confinement. The output of the design process, through which hazards and hazardous situations are identified, control strategies implemented and standards defined will be a set of SSCs that achieve defense in depth. SSCs so identified will always be backed up by administrative controls such as procedures. Administrative controls that afford a measure of defense in depth will be developed prior to facility operations. For the purpose of protecting the public and collocated worker, administrative controls alone shall not be relied on for the implementation of defense in depth. Administrative controls alone may be credited as the controls that protect facility workers, when appropriate. In such cases, defense in depth is provided through other human aspects, such as worker qualification and training.

Internal Safety Reviews

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criterion 7.1-3, requires that the RPP-WTP contractor establish a safety framework and specifies requirements for the Internal Safety Oversight program consistent with Top-Level Principle 4.4.1, "Safety Review Organization". BNI has established a RPP-WTP Project Safety Committee (PSC) to provide an independent, interdisciplinary evaluation of matters related to nuclear, radiological, and process safety.

Operating Limits (Technical Safety Requirements)

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criterion 9.2-1, commits the RPP-WTP contractor to prepare, submit for approval, and operate the facility in accordance with Technical Safety Requirements (TSRs). SCs 9.2-2 through 9.2-6 provide the safety criteria for the bases and contents, updating, submission for regulatory approval, and maintenance of TSRs.

As part of hazard evaluation, the role of the operator in the development of a potential hazard will be identified and reliability assessed. Human factors specialists in the multidisciplinary team will support this evaluation. The results of the assessment will be incorporated into administrative controls such as operating procedures and TSRs.

Worker Qualification and Training

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Section 7.2, commits the RPP-WTP contractor to establish and implement a training program. Consistent with Top-Level Principles 4.3.4.1, "Personnel Training", 4.3.4.2, "Training Programs", and 5.2.4, "Process Safety - Training," SRD Volume II, Section 7 requires that the program address:

- continual training - SC 7.2-1, 7.2-3, 7.3-3
- qualification of personnel - SC 7.3-3
- records of training status - SC 7.2-4
- establishment of written procedures/instructions - SC 7.2-2, 7.2-5

Establishment of a Safety/Quality Program

The Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Safety Criteria 1.0-1, requires the use of a comprehensive safety management program consistent with Top-Level Principle 5.1.1, "Process Safety Management", and 5.1.2, "Process Safety Objective". Safety Criterion 7.1-3 requires a safety framework be established to implement this Program consistent with Top-Level Principle 4.1.4.1, "Safety/Quality Culture".

Establishment of a Quality Program is discussed above under the heading, "Quality Assurance Program".

3.0 Determination of SSCs for the Implementation of Defense in Depth

The standards for prevention, control, and human aspects in Sections 2.2, 2.3, and 2.6 are primarily concerned with defense in depth sub-principles that minimize the potential of hazard initiation. In evaluating accidents that are postulated to occur despite implementation of preventive, control and human aspects, the sub-principles of mitigation and automatic systems must be considered.

The Implementing Standard for Safety Standards and Requirements Identification describes the process by which hazards and hazardous situations are identified and evaluated to determine hazard control strategies. Use of this Implementing Standard ensures that the defense in depth sub-principles are accounted for in the process of determining hazard control strategies. That process will identify SSCs that perform defense in depth as part of their safety function. The administrative controls that back up these SSCs will be developed prior to the introduction of hazardous materials into the facility.

Table 1 is the standard for implementing defense in depth by SSCs as part of the hazard control strategy; it defines the minimum number of SSCs and associated engineering requirements for the control of hazards of a particular severity.

Table 1 will be used in conjunction with the guidance in Section 2.0 to ensure that the preferred control solution addresses the strategies that protect the public and collocated workers; such SSCs will always be backed up by the human aspects of defense in depth discussed in Section 2.6.

The table lists the number and attributes of the physical barriers, as well as the application of the single failure criterion to SSCs that are required to adequately implement defense in depth for a given control strategy. Confirmation of the adequacy of implementation is achieved by meeting the numerical guidance stated in the third column. Consistent with the defense in depth sub-principles in Section 2.0, the control strategy should emphasize passive SSCs over active SSCs.

Hazard severities and target frequencies are the means to achieve adequate defense in depth in accordance with the tailored approach mandated by RL/REG 98-17, "Regulatory Unit Position on Tailoring for Safety."

1st Column - SL (Severity Level)

Determination of hazard severity level is based on an assessment of unmitigated consequences. Severity levels are defined as SL-1 to SL-4, with SL-1 having the highest consequences.

2nd Column - Control Options for Implementation of Defense in Depth

A graded approach is reflected in the configuration requirements against each hazard severity level. The requirements are more stringent for defense in depth implementation for hazards of greater severity than for those of lesser severity.

Implementation of defense in depth requires that the single failure criterion be applied in a tailored fashion. For SL-1, application of the single failure criterion is mandatory. For SL-2, the single failure criterion shall be considered; that is, an objective assessment must be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. The single failure criterion is discussed in Section 2.1.

In addition to the single failure criteria in Table 1, diversity may also be implemented in the control strategy where hazards assessment reveals a common mode failure concern (see the Implementing Standard for Safety Standards and Requirements Identification, SRD Vol. II, Appendix A).

Implementation of defense in depth also requires that the provision of physical barriers be applied in a tailored fashion. In Table 1, provision of physical barriers refers to those that provide confinement against the release of hazardous materials, as opposed to barriers that protect against direct radiation. For SL-1 and SL-2, two or more independent physical barriers are required. For SL-3, at least one physical barrier shall be provided, and two or more independent physical barriers shall be considered; that is, an objective assessment must be performed to determine the extent to which physical barriers will be incorporated by the design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. For SL-4, physical design features and/or administrative controls per 10CFR 835.1001 shall be provided.

The graded approach is also reflected in the degree of confidence required commensurate with the hazard severity. The confidence is based on the standards and other attributes applicable to the particular control strategy. The Implementing Standard for Safety Standards and Requirements Identification describes selection of standards and other attributes applicable to control strategies.

3rd Column - Target Frequency (yr^{-1})

This column lists the target frequencies for each hazard severity level. The hazard severity level is a measure of the consequence from an unmitigated event - that is, an event in which both SSCs that prevent the accident and SSCs that mitigate the accident fail. After the preferred hazard control strategy has been identified, the event frequency - i.e., the product of the frequency of the initiating event and the probability that the control strategy will fail given the initiating event - will be conservatively estimated. (No credit is taken for administrative controls in calculating the initiating event frequency.) Verifying that the event frequency is less than the target frequency will provide confirmation that the chosen control strategy includes sufficient SSCs to adequately implement defense in depth in a graded approach.

The demonstration of having met the target frequencies may be based on either numerical analysis or engineering judgment. When appropriate, administrative controls alone may be credited as the controls that protect facility workers. The hazard assessment and control team shall assess the confidence in the frequency so determined, applying greater conservatism where engineering judgment is employed.

Table 1. Implementation of Defense in Depth by SSCs.

Severity Level	Control Options for Implementation of Defense in Depth	Target Frequency (yr^{-1})
SL-1	Two or more independent physical barriers. The single failure criterion shall be applied.	$< 10^{-6}$
SL-2	Two or more independent physical barriers. The single failure criterion shall be considered.	$< 10^{-4}$
SL-3	At least one physical barrier shall be provided. Two or more independent physical barriers shall be considered.	$< 10^{-2}$
SL-4	Physical design features and/or administrative controls per 10 CFR 835.1001	$< 10^{-1}$

4.0 Definitions

Definitions of the following terms were obtained from the referenced consensus standards. Minor wording differences among multiple references are ignored. In some cases, the definition of a term given in the referenced consensus standard has been tailored to the relative risks of the RPP-WTP and its anticipated associated hazards. Other wording differences in the definitions below from the cited consensus standards have been made to preserve consistency with terminology in other RPP-WTP safety documentation. Such differences are identified by presenting added words in Italics and by inserting double-brackets where words have been removed. Citation of a definition from a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

Active component [SSC]. A component in which mechanical movement must occur to accomplish the [ ] safety function of the component (Ref. 5.5, 5.6)

Active failure. A malfunction, excluding passive failures, of a component that relies on mechanical movement to complete its intended [ ] safety function upon demand

Examples of active failures include the failure of a valve or check valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start.

Spurious action of a powered component originating within its actuation or control system shall be regarded as an active failure unless the specific design features or operating restrictions preclude such spurious action. An example is the unintended energization of a powered valve to open or close (Ref. 5.5, 5.6, 5.8).

Administrative controls. Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of the facility.

Barrier. A control that has the function of maintaining confinement, that is preventing or mitigating the release of radioactive or hazardous material to the worker, public or the environment. This control can be an SSC that provides a physical barrier (e.g. vessel, shielding, and filtration) or an administrative control (e.g. training and procedures), which supplements the physical barriers.

Common cause failure. Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures (Ref. 5.4).

Common mode failure. Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation (Ref. 5.4).

Confinement. Physical barrier that prevents or mitigates the release of radioactive or hazardous material to the worker, public or the environment. The DOE nonreactor facility safety Implementation Guide identifies three kinds of confinement barriers - primary confinement, secondary confinement, and tertiary confinement (Ref. 5.3).

Control strategy. A set of generally-described provisions (barriers, dilution/dispersal, physical limitations on material quantities, administrative material controls, confinement, ventilation of flammable gas, etc.) and/or approaches (defense in depth, use of passive features, prevention, mitigation, etc.) which are intended to assure adequate control of a specific hazard and associated accidents in the context of the work (Ref. 5.4).

Defense in depth. The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or the environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualifications and training and safety program. Design provisions including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public or the environment (Ref. 5.4).

Design Basis Events. Postulated events providing bounding conditions for establishing the performance requirements of structures, systems and components that are necessary to: 1) ensure the integrity of the safety boundaries protecting the worker; 2) place and maintain the facility in a safe state indefinitely; or 3) prevent or mitigate the event consequences so that the radiological exposures to the general public or the workers would not exceed appropriate limits. The Design Basis Events also establish the performance requirements of the structures, systems, and components whose failure under Design Basis Event conditions could adversely affect any of the above functions (Ref. 5.4).

Detectable failures. [The following definition is considered to be specific to electrical, instrumentation and control systems.]

> Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication (Ref. 5.9).

Diversity. Use of different technologies, equipment, or design methods to perform a common function with the intent to minimize common cause failures (Ref. 5.13).

Engineered feature. A structure, system or component that contributes to the safe operation of the facility (Ref. 5.14).

Event. A condition that deviates from normal operation, i.e., an initiating occurrence plus single failure or coincident occurrence combination (Ref. 5.5, 5.6).

External Event. An event external to the RPP-WTP caused by (1) a natural hazard (e.g., earthquake, flood, lightning, or range fire) or (2) a human-induced event (e.g., transportation or nearby industrial activity).

Human factors engineering (HFE). An interdisciplinary science and technology concerned with the process of designing for human use (Ref. 5.12).

Important to Safety. Structures, systems and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems and components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems and components should be considered for inclusion within this definition (Ref. 5.4).

Independence. The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable (Ref. 5.10).

Initiating occurrence/event. A single occurrence and its consequential effects that place the plant or some portion of the plant in an off-normal condition. An initiating occurrence/event is not the single failure defined elsewhere herein. An initiating occurrence can be *an internal event or an external event* (Ref. 5.5, 5.6, 5.8).

The first event in an event sequence. Can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident (Ref. 5.15).

Internal Event. An occurrence related to structure, system, and component performance or human action, or an occurrence external to the system but within the RPP-WTP that causes upset of a structure, system, or component.

Limiting design requirements. The limiting value of a design parameter that ensures that the consequences of any event do not result in:

- Violation of plant nuclear safety criteria, including off-site radiological dose criteria, or
- Unacceptable degradation of plant components that are required to mitigate the consequences of an event.

(A single event may have more than one limiting design requirement.) (Ref. 5.7)

Long term. *For fluid systems*, the long term is defined as that period of *important to safety* fluid system operation following the short term during which the safety function of the system is required (Ref. 5.8).

Passive component. A component that is not an active component (Ref. 5.5, 5.6).

Passive failure. The blockage of a process flow path or failure of a component to maintain its structural integrity or stability, such that it cannot provide its intended [ ] safety function upon demand (Ref. 5.5, 5.6, 5.8).

Primary confinement. Provides confinement of hazardous material to the vicinity of its processing. This confinement is typically provided by piping, tanks, glove boxes, encapsulating material, and the like, along with any offgas systems that control effluent from the primary confinement (Ref. 5.3).

Redundant equipment or system. A system or component that duplicates the essential functions of another system or component to the extent that either may perform the required function, regardless of the state of operation or failure of the other (Ref. 5.9, 5.10).

Safety function. Any function that is necessary to ensure: 1) the integrity of the boundaries retaining the radioactive materials; 2) the capability to place and maintain the facility in a safe state; or 3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits (Ref. 5.4).

Secondary confinement. Consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area. Except in the case of housing glove-box operations, the area inside this barrier is usually unoccupied (e.g., canyons, hot cells); it provides protection for operating personnel (Ref. 5.3).

Shall, should and may. The word “shall” is used to denote a requirement; the word “should” is used to denote a recommendation; and the word “may” is used to denote permission, neither a requirement nor a recommendation (Ref. 5.5, 5.6, 5.8).

The word “shall” denotes actions that must be performed… The word “should” is used to indicate recommended practice (Ref. 5.3, based on DOE-STD-1075-94).

Shall [be] consider[ed]. An objective assessment must be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. (Ref. 5.16).

Short term. *For fluid systems*, the short term is defined as that period of operation up to 24 hours following an initiating event [ ] (Ref. 5.8).

Single failure. A random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended [ ] safety function(s) (Ref. 5.5, 5.6).

Single failure criterion. [Two definitions are provided below. The following definition applies to fluid (i.e., liquid and gas) systems.]

> Fluid [ ] systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly), nor (2) a single failure of any passive component (assuming active components function properly) results in a loss of the capability of the system to perform its [ ] safety function (Ref. 5.5, 5.6).

[The following statement of the "single failure criterion" applies to electrical and instrumentation and control systems.]

> The *important to* safety systems shall perform all required safety functions for a design basis event in the presence of the following:
>
> 1. Any single detectable failure within the *important to* safety systems concurrent with all identifiable but non-detectable failures
> 2. All failures caused by the single failure
> 3. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function
>
> The single failure could occur prior to, or at any time during, the design basis event for which the *important to* safety system is required to function (Ref. 5.9).

5.0 References

5.1 10 CFR 830.120, Quality Assurance Requirements

5.2 DOE O 420.1, Facility Safety, Chg 2, 10/24/96

5.3 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria, Rev. G (Draft), September 1995

5.4 DOE/RL-96-0006, Revision 1, Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors

5.5 ANSI/ANS-51.1-1983, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. American Nuclear Society

5.6 ANSI/ANS-52.1-1983, Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants. American Nuclear Society

5.7 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions. American Nuclear Society

5.8 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems. American Nuclear Society

5.9 IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems. IEEE Power Engineering Society

5.10 IEEE Std 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits. IEEE Power Engineering Society

5.11 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. IEEE Power Engineering Society

5.12 IEEE Std 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.

5.13 ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries. Instrument Society of America.

5.14 Integrated Safety Management Plan. 24590-WTP-ISMP-ESH-01-001. Bechtel National, Inc., Richland, WA

5.15 Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples. Center for Process Chemical Safety, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1992.

5.16 DOE O 6430.1A, General Design Criteria, 6 April 1989

6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth

The following subsections summarize the RPP-WTP contractor's tailoring of the consensus standards invoked by this Implementing Standard for Defense in Depth.

6.1 DOE O 420.1, Facility Safety (Ref. 5.2)

Terminology

- Section 4.1.1.2, 1st paragraph, last sentence: Phrase "…workers, including those at adjacent facilities…" is interpreted for RPP-WTP to mean "…workers and collocated workers…"

Applicability

- The only portion of DOE O 420.1 that is being invoked by this Implementing Standard for Defense in Depth is Section 4.1.1.2, the first three paragraphs.

6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3)

Terminology

- By virtue of cross-references within the DOE Implementation Guide (IG), reference is made to "safety class" and "safety significant" SSCs. The RPP-WTP project uses the term "important to safety", which encompasses both "safety class" and "safety significant".
- "Critical safety function" in the DOE IG is interpreted to more broadly read "…significant public, worker and collocated worker impact".

Applicability

- The only portion of the DOE "420.X" Implementation Guide that is being invoked by this Implementing Standard for Defense in Depth is Section 2.3, except the last paragraph.
- Section 2.3 of the DOE IG contains internal cross-references to subsections 5.2.1, 5.2.2.1 and 5.2.2.2, which list typical codes for structures, ventilation systems, and process equipment that provide a confinement function. Section 2.4.2 of this Implementing Standard lists the SRD Safety Criteria that will be applied to SSCs comprising confinement.
- Section 2.3 of the DOE IG contains an internal cross-reference to subsection 5.2.1, which further cites section 4.4 of DOE O 420.1 and section 3.3 of the DOE IG for criteria for natural phenomena hazards (NPH). For the RPP-WTP, NPH criteria are provided in SRD Safety Criteria SC 4.1-3 and SC 4.1-4.

6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

Terminology

- "Safety-related" is interpreted for RPP-WTP to mean "important to safety" or "ITS".
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function" as defined in DOE/RL-96-0006, Rev. 1.

Non-Applicability

- Assumption (1) of section 1.3 does not apply. Single failure criteria for the RPP-WTP project are given in the consensus standards invoked and tailored by this Implementing Standard (ANSI/ANS-58.9-1981 and IEEE 379-1994).
- Assumption (4) of section 1.3 does not apply. The operators will be qualified in accordance with the RPP-WTP training program, per Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Section 7.2.
- "Automatic reactor trip…" does not apply.

6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)

Terminology

- "Containment" or "containment vessel" is interpreted to mean "confinement".
- "Seismic Category I standards" is interpreted as seismic requirements for a SSC with a seismic safety function per SRD Volume II (24590-WTP-SRD-ESH-01-001-02) Safety Criterion 4.1-3 for the RPP-WTP.
- "Safety related" is interpreted for RPP-WTP to mean "important to safety" or "ITS". Conversely, "non-safety-related" means "non-ITS".
- "Technical specification(s)" is interpreted to mean "Technical Safety Requirements" or "TSR(s)".
- "Condition I" is interpreted for RPP-WTP to mean "normal operation".
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function" as defined in DOE/RL-96-0006, Rev. 1.
- In definition of "single failure", reference [1] does not apply to RPP-WTP.
- Safety classes 1, 2, and 3 (section 4.5) are interpreted to be important to safety systems.

Non-Applicability

- For RPP-WTP, the need for emergency onsite power will be ascertained in accordance with the DOE/RL-96-0004 process as part of determining hazard control strategies.
- In the definition of "short term" (section 2), everything after "…up to 24 hours following an initiating event" applies to nuclear power reactor plants and is therefore not applicable to RPP-WTP.
- Sections 3.1 through 3.3 of ANSI/ANS 58.9 are not applicable to the RPP-WTP. Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Reactor-specific regulations (e.g., 10 CFR 50 Appendix A) are not applicable to RPP-WTP (see Section 1, 1st paragraph).
- References to a reactor "unit", "safe shutdown", and "loss of coolant accident" are nuclear reactor plant-specific and, therefore, do not apply to RPP-WTP.
- Sections 3.1 through 3.3 are reactor-specific and do not apply to RPP-WTP.

6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

Terminology

- BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:
  - Common-cause failure
  - Design basis events
  - Safety function
- "Safety system" is interpreted for RPP-WTP to mean "important to safety system". Consequently, "important to safety system" is interpreted to mean a system that performs a safety function, as defined in DOE/RL-96-0006.
- "Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.

Applicability

- Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Nuclear reactor plant-specific terms such as reactor "unit", "reactor trip system" power, control rods, "safety injection", "core spray", and "low pressure coolant injection" do not apply to RPP-WTP.

6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)

Terminology

- The definition of "administrative controls" in section 2 of the consensus standard is understood as being consistent with the definition given in section 4.0 of this Implementing Standard.
- The definition of "Class 1E" is interpreted for the RPP-WTP as follows: "The classification of the electric equipment and systems that perform a safety function." The note following the definition of "Class 1E" in the consensus standard is retained for RPP-WTP.
- BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:
  - Design basis events
  - Safety function
- "Safety system" is interpreted for RPP-WTP to mean "important to safety system". Consequently, "important to safety system" is interpreted to mean a system that performs a safety function, as defined in DOE/RL-96-0006.
- "Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.
- "Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.

Non-Applicability

- Nuclear reactor plant-specific terms such as reactor "unit", "emergency reactor shutdown", "reactor heat removal", do not apply to RPP-WTP.

6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12)

Terminology

- "Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.

Non-Applicability

- Application of the formal human factors engineering process described in subsection 6.1.1 of IEEE Std 1023-1988 is tailored to the work and hazards presented by the RPP-WTP in subsection 2.6.2 of this Implementing Standard.

- Section 6.1.1.12 and 6.1.1.18 of IEEE Standard 1023-1998 recommends the use of a separate plant simulator or physical mockup for human factors engineering. As discussed in subsection 2.6.2 of this Implementing Standard, the RPP-WTP contractor does not currently plan to construct a separate plant simulator or physical mockup and these sections are, therefore, not applicable to RPP-WTP.

6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13)

Terminology

- The definition of "common-cause failure" given in DOE/RL-96-0006 is used, rather than that in section 3 of the consensus standard.
- "Safety Instrumented System (SIS)" is interpreted to refer to any instrumentation and control system in the RPP-WTP that is important to safety, as defined in DOE/RL-96-0006.

Appendix C

Implementing Standards

CONTENTS

Section Implementing Standard **Page**

1.0 ISO 10007, Quality Management - Guidelines for Configuration Management C-1

2.0 DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities" C-3

3.0 ANSI/AISC N690, "Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities" C-12

4.0 DOE G-420.1/G-440.1, Implementation Guide for Use with DOE Orders 420.1 and 440.1, Fire Safety Program C-13

5.0 DOE-STD-1066-97, Fire Protection Design Criteria C-14

6.0 NFPA 801, Standard for Facilities Handling Radioactive Materials C-16

1.0 ISO 10007, Quality Management - Guidelines for Configuration Management

Revision: First Edition, April 15, 1995
Sponsoring Organization: International Organization for Standardization

RPP-WTP Specific Tailoring

The following tailoring of ISO 10007 is required for use by the RPP-WTP contractor as an Implementing Standard for Configuration Management.

Page 1, Section 1 Scope

Second paragraph, last sentence. Replace this sentence with:

"For RPP-WTP ISO 10007 amplifies on the configuration management elements found in the Quality Assurance Program, BNFL-5193-QAP-01."

Justification: For RPP-WTP the approved QAP defines the quality management and quality system elements.

Page 1, Section 2 Normative References

Delete reference to the ISO 10011 series of standards.

Justification: As discussed for Section 8, for RPP-WTP the approved QAP defines the principles, criteria, and practices for the configuration management system audit.

Page 7, Section 7.7 Configuration Management Plant (CMP)

Delete second paragraph

Justification: This paragraph addresses activities outside the RPP-WTP project workscope or control (i.e., multiple projects, multi-level contracts, and customer configuration management plans).

Page 8, Section 8 Configuration Management System Audit

Revise the last paragraph to read:

"Principles, criteria, and practices of the CM system audit should comply to the RPP-WTP QAPIP."

Justification: For RPP-WTP the approved QAP defines the principles, criteria, and practices for the conduct of audits and self-assessments.

Page 11 and 12, Annex B

Delete.

Justification: Although provided only as information, as noted in Section 1 above, the ISO 9000 Series of Standards are not being implemented at RPP-WTP and this Annex is therefore removed to reduce potential confusion to non-applicable cross references.

2.0 DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities"

Revision: Change Notice #1 dated 1/96 and DOE Newsletter dated 1/22/98 (Interim Advisory on Straight Winds and Tornados)

Sponsoring Organization: DOE

RPP-WTP Specific Tailoring

The following tailoring of DOE-STD-1020-94 is required for use by the RPP-WTP contractor as an Implementing Standard for seismic analysis and design.

Page 1-6, Section 1.3 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 2-1, Section 2.2 General Approach for Seismic Design and Evaluation

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page 2-6, Section 2.3 Seismic Design and Evaluation of Structures, Systems, and Components

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 2-8, Section 2.3.1 Performance Category 1 and 2 Structures, Systems, and Components

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 2-12, Section 2.3.2 Performance Category 3 and 4 Structures, Systems, and Components

Disregard the requirements for PC-4 SSCs.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use ACI 349 for design of reinforced concrete in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Use ANSI/AISC N690 for design of structural steel in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Page 2-15, Section 2.3.3 Damping Values for Performance Category 3 and 4 Structures, Systems, and Components

Use ASME Code Case N-411 damping value for piping in lieu of those shown in Table 2-3.

Justification: This value is acceptable to the NRC for nuclear power plants.

Page 2-18, Section 2.4.1 Equipment and Distribution Systems

Perform seismic design of PC-1 and -2 elements of structures and equipment per the provisions of 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 2-22, Section 2.4.2 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 2-24, Section 2.5 Summary of Seismic Provisions

Disregard the requirements for PC-4 SSCs.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Use the seismic provisions in Table 2-5 concerning PC-3 SSCs except that the structural capacity is to be based on code ultimate strength or allowable behavior level.

Justification: Limit-state level method of determining the structural capacity is more appropriate for evaluation of existing facilities (the RPP-WTP is a new facility).

Page 3-1, Section 3.1 Introduction

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 3-2, Section 3.2 Wind Design Criteria

Use peak gust speed values contained in Attachment "A" of DOE Interim Advisory dated 1/22/98 in lieu of fastest-mile wind speeds shown in Table 3-2; also, per DOE Interim Advisory, use an importance factor for PC-2 SSCs of 1.0 in lieu of 1.07 indicated in Table 3-1.

Justification: The Newsletter was issued by DOE as an interim measure for use with DOE-STD-1020-94 until such time as the standard is revised.

Page 3-5, Section 3.2.1 Performance Category 1

Design structural steel PC-1 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred to the UBC because it is a national consensus code.

Design reinforced concrete PC-1 structures per ACI 318-99.

Justification: The ACI 318 code is preferred to the UBC because it is a national consensus code.

Page 3-6, Section 3.2.2 Performance Category 2

Design structural steel PC-2 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred to the UBC because it is a national consensus code.

Design reinforced concrete PC-2 structures per ACI 318-99.

Justification: The ACI 318 code is preferred to the UBC because it is a national consensus code.

Page 3-6, Section 3.2.3 Performance Category 3

Design structural steel PC-3 structures per ANSI/AISC N690-94.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Design reinforced concrete PC-3 structures per ACI 349-97.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Disregard requirements for tornado design.

Justification: Tornado is not a credible NPH at the RPP-WTP site.

Page 3-11, Section 3.2.4 Performance Category 4

Delete this section.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Page 3-13, Section 3.3 Evaluation of Existing SSCs

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 4-1, Section 4.0 Flood Design and Evaluation Criteria

Disregard criteria for the design of SSCs for river flooding.

Justification: River flooding is not a credible NPH at the RPP-WTP site, and only the criteria dealing with local precipitation that affects roof design and site drainage are applicable to the RPP-WTP design.

Page 4-4, Section 4.1.2 Flood Evaluation Process

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page 4-12, Section 4.2.4 Performance Category 4

Delete this section.

Justification: There are no PC-4 SSCs at the RPP-WTP.

Page 4-13, Section 4.3.3 Site Drainage and Roof Design

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page 4-15, Section 4.4 Considerations for Existing Construction

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page 4-16, Section 4.5 Probabilistic Flood Risk Assessment

Do not perform a probabilistic flood risk assessment of the RPP-WTP site.

Justification: UCRL-21069, "Probabilistic Flood Hazard Assessment for the N Reactor, Hanford, Washington", July 1988, contains a probabilistic flood risk assessment of the N reactor site. The RPP-WTP site is close to the N Reactor site (about 10 miles away) and further away from the Columbia River. Therefore, the N Reactor flood assessment may be used and no assessment of the RPP-WTP site is required.

Page B-4, App. B, Section B.2 Graded Approach, Performance Goals, and Performance Categories

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page B-8, App. B, Section B.3 Evaluation of Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page C-1, App. C, Section C.1 Introduction

Perform performance categorization of SSCs per SRD Safety Criteria 4.1-3 and 4.1-4 in lieu of DOE-STD-1021-93.

Justification: DOE-STD-1021-93 is inconsistent with the top-level safety principles in DOE/RL-96-0006. The functions of this standard are implemented by SRD Safety Criteria 4.1-3 and 4.1-4 and Appendix A to Volume II of the SRD.

Page C-19, App. C, Section C.3.2 Earthquake Ground Motion Response Spectra

Disregard Section C.3.2.1 discussion and Table C-4. Follow 1997 UBC for the RPP-WTP design.

Justification: Section C.3.2.1 discussion and Table C-4 are based on 1994 UBC; the 1997 UBC is more current.

Page C-27, App. C, Section C.4 Evaluation of Seismic Demand (Response)

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page C-29, App. C, Section C.4.1 Dynamic Seismic Analysis

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page C-31, App. C, Section C.4.2 Static Force Method of Seismic Analysis

Use 1997 UBC in lieu of 1994 UBC.

Justification: 1997 UBC is more current.

Page C-32, App. C, Section C.4.3 Soil-Structure Interaction

Use ASCE 4-98 (Draft) in lieu of ASCE 4-86.

Justification: ASCE 4-98 (Draft) is more current.

Page C-38, App. C, Section C.4.4 Analytical Treatment of Energy Dissipation and Absorption

Design PC-3 (Seismic Category I) SSCs for the elastic seismic response to DBE per Section 3.7.2 of NRC NUREG-0800, Rev. 3 (Draft) with no credit for inelastic energy absorption. Note: Credit for inelastic energy absorption is allowed in the design of PC-3 (Seismic Category II) SSCs.

Justification: This change is made for consistency with NRC acceptance criteria.

Page C-52, App. C, Section C.5.1 Capacity Approach

Use ACI 349 for design of reinforced concrete in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Use ANSI/AISC N690 for design of structural steel in lieu of UBC.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Page C-62, App. C, Section C.7 Special Considerations for Existing Facilities

Delete this section.

Justification: This section deals with existing facilities and the RPP-WTP is a new facility.

Page C-66, App. C, Section C.9 Alternate Seismic Mitigation Measures

Delete this section.

Justification: Seismic base isolation is not planned to be used in the RPP-WTP design.

Page D-3, App. D, Section D.3 Load Combinations

Design structural steel PC-1 and PC-2 structures per AISC Manual of Steel Construction, Allowable Stress Design, Ninth edition.

Justification: The AISC code is preferred because it is a national consensus code.

Design reinforced concrete PC-1 and PC-2 structures per ACI 318-99.

Justification: The ACI 318 code is preferred because it is a national consensus code.

Design structural steel PC-3 SSCs structures per ANSI/AISC N690-94.

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

Design reinforced concrete PC-3 SSCs structures per ACI 349-97

Justification: This change is made for consistency with NRC acceptance criteria contained in Section 3.8.4 of NUREG-0800, Rev. 2 (Draft).

3.0 ANSI/AISC N690, "Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities"

Revision: 1994
Sponsoring Organization: American National Standards Institute/American Institute of Steel Construction

RPP-WTP Specific Tailoring

The following tailoring of ANSI/AISC N690 is required for use by the RPP-WTP contractor as an Implementing Standard for structural design.

Page 22, Section Q1.5.7.1 Primary Stresses

Revise the stress limit coefficients for compression in Table Q1.5.7.1 as follows:

- 1.3 instead of 1.5 [stated in footnote (c)] in load combinations 2, 5, and 6
- 1.4 instead of 1.6 in load combinations 7, 8, and 9
- 1.6 instead of 1.7 in load combination 11

Justification: These changes are made for consistency with the NRC requirements of Appendix F of Section 3.8.4 of NUREG-0800 (Draft Rev. 2).

Page 22, Section Q1.5.7.1 Primary Stresses

Delete the following load combinations:

4. D + L + Eo
6. D + L + Ro + To + Eo

Justification: These load combinations are requried for evaluation of an Operation Basis Earthquake (OBE). The WTP project has not identified an OBE event.

4.0 DOE G-420.1/G-440.1, Implementation Guide for Use with DOE Orders 420.1 and 440.1, Fire Safety Program*

Revision: September 30, 1995

Sponsoring Organization: U. S. Department of Energy

RPP-WTP Specific Tailoring

The following tailoring of DOE G-420.1/G-440.1 is required for use by the RPP-WTP Project as an implementing standard for fire safety.

Section III.5.0

Add the following words at the end of the paragraph: "The applicable building code for the RPP-WTP Project is the 1997 Uniform Building Code (UBC)."

Justification: To clarify that the code in effect at the time that facility design commenced was the 1997 UBC.

Section III.6.3

Revise to read "Automatic fire extinguishing systems in all areas subject to loss of safety class systems, significant life safety hazards, or unacceptable program interruption. The FHA may justify the omission of such systems based on safety considerations as approved by the AHJ.

Justification: The addition is consistent with governing Safety Criterion 4.5-4, which requires automatic fire suppression "unless the Fire Hazards Analysis dictates otherwise". It is also consistent with the DOE equivalency concept described in DOE G-420.1/G-440.1 Section II.

Section IV.4.5

Change "Description of critical process equipment" to "Identification of Important-To-Safety Equipment".

Justification: The term "critical process equipment" is not well defined for the RPP-WTP Project. By contrast the term "Important-to-Safety" is defined by the DOE regulatory documents, such as DOE/RL-96-0004. Identification of Important-to-Safety equipment is more meaningful and is consistent with the CAR Guidance (RL/REG-99-05).

5.0 DOE-STD-1066-97, Fire Protection Design Criteria

Revision: March 1997

Sponsoring Organization: U. S. Department of Energy

RPP-WTP Specific Tailoring

The following tailoring of DOE-STD-1066-97 is required for use by the RPP-WTP Project as an implementing standard for fire safety.

Section 9.5.1

Add the following words: "The fire resistance of special or unique penetration assemblies, such as lead glass windows and shield wall penetrations, may be based on past qualification testing or an equivalency evaluation."

Justification: The RPP-WTP facility is expected to have unique penetration configurations that may be impractical to test. This change clarifies that alternate approaches that provide a comparable level of safety, as described in Section 1 of DOE-Std-1066-97, may be used.

Section 10.4

Add the following words: "The 75-foot travel distance may be exceeded in areas not normally occupied by personnel, where plant equipment alone is located".

Justification: If an area is not normally occupied an accidental breach of a primary confinement system cannot expose personnel to radioactive material.

Section 10.6.3:

Delete the statement that: "In addition, for explosives environments, exits should reflect the criteria contained in the DOE Explosives Safety Manual (DOE M 440.1-1)."

Justification: The DOE Explosives Safety Manual applies to environments involving munitions, and is not applicable to the RPP-WTP.

Section 11.4

Revise this section to read: "Where required by the SAR, critical facilities should be served by dedicated, redundant electric power services. External to the buildings served, the two services should be separated by 4-hour fire-rated construction and should be served from separate sources.

Justification: The term "power services" is more consistent with the sentence that follows. The changes clarify that the requirement applies to site power supplies, not to cable routing within the buildings served.

Section 12.4

Delete this section.

Justification: This section is not applicable because there will be no gas-fired process furnaces in the RPP-WTP.

Section 13

Delete all except Subsection 13.1

Justification: The RPP-WTP is not a Plutonium Processing and Handling Facility, a Plutonium Storage Facility, an Enriched Uranium Storage Facility, a Uranium Processing and Handling Facility, a Fuel Reprocessing Facility, or a Uranium Conversion and Recovery Facility.

6.0 NFPA 801, Standard for Facilities Handling Radioactive Materials

Revision: 1995 edition

Sponsoring Organization: National Fire Protection Association

RPP-WTP Specific Tailoring

The following tailoring of NFPA 801-95 is required for use by the RPP-WTP project as an implementing standard for fire safety.

Section 3-8

Replace entire section with the text of the same section from the 1998 version of NFPA 801.

Justification: The NFPA standard was revised in recognition of the impracticality of using only noncombustible surface finishes in areas processing or storing radioactive materials. Conformance with the revised standard will permit the use of limited combustible interior finishes.

Section 6.1.1

Change the code edition for NFPA 70 from 1993 to 1996 and the code edition for NFPA 780 from 1992 to 1995.

Justification: SRD safety criteria 4.3-2 and 4.4-12 reference these more recent editions of NFPA 70 and NFPA 780 as implementing standards. This change resolves the conflict with NFPA 801.

7.0 ACI 349, Code Requirements for Nuclear Safety-Related Concrete Structures

Revision: 2001
Sponsoring Organization: American Concrete Institute

WTP Specific Tailoring

The following tailoring of ACI 349-01 is required for use by the WTP contractor as an implementing standard for structural design.

Chapter 21

Replace Chapter 21 of ACI 349-01 with Chapter 21 of ACI 318-99.

Justification: Chapter 21 of ACI 349-01 is based on criteria from ACI 318-95. The American Concrete Institute completed a major revision of ACI 318 between the years 1995 and 1999 with respect to seismic proportioning and detailing. The WTP project wishes to adopt the most current methodology as presented in ACI 318-99 in lieu of that presented in ACI 349-01 Chapter 21.

8.0 ACI 318, Building Code Requirements for Structural Concrete and Commentary

Revision: 1999
Sponsoring Organization: American Concrete Institute

WTP Specific Tailoring

The following tailoring of ACI 318-99 is required for use by the WTP contractor as an implementing standard for design of reinforced concrete for Seismic Category III SSCs, as noted.

Chapter 9, Section 9.2 Required Strength

The following additional load combinations from the *Uniform Building Code*, 1997, section 1612.2.1, shall be included in the load combinations evaluated for design of reinforced concrete:

Equation (12-5): $1.2D + 1.0E + (f_1L + f_2S)$

Equation (12-6): $0.9D \pm (1.0E \text{ or } 1.3W)$

Justification: The additional load combinations implemented are not identified in the ACI load combinations. These combinations are evaluated to ensure adequate equivalency with commercial design in accordance with the UBC.

Chapter 21, Section 21.2.1.3

Seismic detailing requirements for "moderate seismic risk" will be used.

Justification: The "moderate seismic risk" classification is consistent with the Seismic Category III, which is an important facility in seismic zone 2B.

General (no specific chapter)

Design of concrete anchorage will follow the requirements of PCA Publication EB 080.01, *Strength Design of Anchorage to Concrete*.

Justification: This design standard represents the current industry approach to design of concrete embedments. This design method has been adoped by ACI 349, committee and used in the 2001 edition for Appendix B. The load factors are lower than those identified for safety related structures applicable to higher seismic classification. The load factors in this publication are appropriate for use in important commercial structures commensurate with SC-III.

9.0 AISC M016, Manual of Steel Construction, Allowable Stress Design (ASD)

Revision: 9th Edition
Sponsoring Organization: American Institute of Steel Construction

WTP Specific Tailoring

The following tailoring of M016 is required for use by the WTP contractor as an implementing standard for design of structural steel for Seismic Category III SSCs.

No specific section

Load combinations for design of structural steel members utilize those identified in UBC 97, section 1612.3.

Justification: These load combinations represent the commercial requirements for allowable stress design of structural steel. Use of these load combinations will ensure compliance with the commercial design in accordance with the UBC.

No specific section

Seismic detailing requirements shall be in accordance wioth UBC 97, Chapter 22, Division V, section 2214, for moderate seismic risk structures.

Justification: The requirements contained in this section contain accepted industry practice for design of important commercial steel structures. Use of this section will ensure compliance with the commercial design in accordance with the UBC.

10.0 UBC 97, Uniform Building Code

Revision: 1997
Sponsoring Organization: International Conference of Building Officials

WTP Specific Tailoring

The following tailoring of UBC 97 is required for use by the WTP contractor as an implementing standard for design of reinforced concrete for Seismic Category III SSCs, as noted.

Division II Snow

Design for snow loads shall be in acordance with ASCE 7, *Minimum Design Loads for Buildings and Other Structures*, section 7.0, utilizing ground snow loads identified in Safety Criterion 4.1-4.

Justification: This approach to design of snow loads is an acceptable industry practice for evaluation of structures under snow loads. This code is more thorough in its consideration of these loads than the UBC methodology.

Division III Wind

Design for wind loads shall be in accordance with ASCE 7, *Minimum Design Loads for Buildings and Other Structures*, section 6.0, utilizing 3-second gust values identified in Safety Criterion 4.1-4.

Justification: This approach to design of wind loads is an acceptable industry practice for evaluation of structures under wind loads. This code is more thorough in its consideration of these loads than the UBC methodology.

Appendix D

Radiological Exposure Standards for the RPP-WTP Project

CONTENTS

1.0 Introduction and Purpose D-1
2.0 Exposure Standards for Facility and Collocated Workers D-2
3.0 Development of the BNI Approach to Compliance with Table 1 of DOE/RL-96-0006 ..... D-5
3.1 Estimated Frequency of Occurrence D-5
3.2 Normal Events/Public and Workers Exposure Standards D-5
3.3 Anticipated Events/Worker and Collocated Worker Exposure Standards D-6
3.4 Extremely Unlikely Events/Public Exposure Standard D-7
3.5 Location of Receptors D-7
3.5.1 Facility Worker D-7
3.5.2 Collocated Worker D-9
3.5.3 Public D-9
4.0 References D-12

1.0 Introduction and Purpose

This attachment to the SRD originally was issued as a stand-alone document (BNFL-5193-RES-01, Rev. 0, dated August 28, 1997). It has been incorporated into the SRD because it provides both background information and the basis for the radiological exposure standards reflected in the SRD Safety Criteria. In addition, it has been updated to reflect responses to DOE questions on the Standards Approval Package.

This document is the Radiation Exposure Standard for Workers Under Accident Conditions, which is a radiological safety deliverable. This document is used during the process hazards analysis (PHA) and accident analysis to ensure worker safety through identification of the need for accident prevention and mitigation features that provide worker protection against radiological and nuclear hazards. In this document, where unmodified reference is made to workers, it applies collectively to facility workers and collocated workers as defined in Sections 3.5.1 and 3.5.2 below.

The U.S. Department of Energy (DOE), in DOE/RL-96-0006, Revision 0, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, (DOE-RL 1996), provides Table 1, "Dose Standards Above Normal Background". In Table 1 (referred to as DOE Table 1), there are entries labeled, "To be derived", for which the contractor is to propose specific exposure standards for both facility workers and collocated workers for the following events:

- **Unlikely Events**: events that are not expected but may occur during the lifetime of the facility in the range of frequency between 10^{-2}/yr and 10^{-4}/yr (between once in 100 years and once in 10,000 years)
- **Extremely Unlikely Events**: events that are not expected to occur during the lifetime of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material. Extremely unlikely events are in the range of frequency between 10^{-4}/yr and 10^{-6}/yr (between once in 10,000 years and once in 1 million years).

This document provides the required exposure standards and the bases for their selection. In addition, this document presents the approach for complying with DOE Table 1. The individual elements of this approach, as shown in Table 2-1 of SRD Safety Criterion 2.0-1 (referred to as Table 2-1), are conservative based on the requirements of the contract and, as such, satisfy the contract. For completeness, this document also discusses, and presents in Table 2-1, public exposure standards and the assumed locations of the public, facility worker, and collocated worker for use in evaluation of accident consequences and normal radioactive material releases.

2.0 Exposure Standards for Facility and Collocated Workers

The four "To be derived" cells in DOE Table 1 have been completed by imposing a radiological exposure standard not to exceed 25 rem/event to the RPP-WTP facility workers or to collocated workers for either unlikely or extremely unlikely events.

The 25 rem/event exposure standard for both the facility and collocated workers for unlikely and extremely unlikely events corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2×10^{-2}. For unlikely events (defined in Table 2-1 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of only 2×10^{-4}, which is considerably less than the average accidental death risk for workers in some of the safest industries (i.e., retail and wholesale trade, manufacturing, and service [EPA 1991]).

Compliance with the 25 rem/event standard is established using qualitative methods supported, where necessary, by numerical analysis that may include the development of event trees and fault trees and/or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls are identified.

Use of qualitative methods is consistent with the American Institute of Chemical Engineers (AIChE) guidelines (AIChE 1992), U.S. Nuclear Regulatory Commission (NRC) guidance for the performance of integrated safety analysis for 10 *Code of Federal Regulations* (CFR) 70 special nuclear material licensees (NRC 1995a), as well as DOE-STD-3009 (DOE 1994) and DOE G 420.1-X (DOE 1995). Both DOE documents state the following:

> "Estimates of worker consequences for the purpose of a safety-significant SSC designation are not intended to require detailed analytical modeling. Considerations should be based on engineering judgement of possible effects and the potential added value of safety-significant SSC designation."

Because the primary purpose of the RPP-WTP Project facility and collocated worker exposure standards is to identify structures, systems, and components (SSC) required to protect these workers, the guidance cited above is both applicable and appropriate.

The principal approach for complying with the 25 rem/event worker exposure standard is the PHA. The PHA is a systematic, team-based review of the plant and treatment processes. The PHA identifies hazards and operability problems to a level of detail commensurate with the design detail available. Further hazard evaluation takes place in parallel with design development to ensure that safety continues to be built into the design process.

Having generated the list of hazards and hazardous situations, this list is subject to a further systematic team-based review where a binning process takes place. The binning process assigns postulated events to a certain hazard category and is essentially risk-based with categories of hazard defined according to a frequency/consequence matrix.

The 25 rem/event standard for unlikely or extremely unlikely events applies to events with frequencies less than 10^{-2}/yr. For those frequencies, the PHA process assigns serious and major hazardous situations as undesirable, acceptable with controls, or acceptable. For a hazardous situation to be "acceptable", its consequences must be less than 25 rem. Where there is uncertainty as to where an event should be binned (i.e., assigning a hazard category), it is binned into a higher category to ensure that the accident analysis remains conservative.

The DOE-RU has provided a guidance document (DOE-RL 1997) to be used for review of the Radiation Exposure Standard for Workers Under Accident Conditions. This guidance document includes the worker accident risk goal and the accident risk goal of DOE/RL-96-0006.

The worker accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to workers in the vicinity of the Contractor's facility, of fatality from radiological exposure that might result from an accident should not be a significant contributor to the overall occupational risk of fatality to workers".

DOE/RL-97-09 (DOE-RL 1997) describes approaches that can be taken to meet this goal. The simplest approach notes that the goal can be met when (a) a worker dose standard that does not exceed 100 rem is used for extremely unlikely events (10^{-4} to 10^{-6} probability range), and (b) a worker dose standard that does not exceed 10 rem is used for unlikely events (10^{-2} to 10^{-4} probability range). For the latter probability range, the 10-rem standard relies on the assumption that the probability of accidents is evenly distributed across the probability range.

Based on experience with similar plants, it is considered unlikely that the even distribution assumption will represent the actual situation for RPP-WTP. Furthermore, experience indicates that there will be relatively few accidents falling into this range, and that they will be distributed toward the low probability end of the range. Consequently, a value higher than 10 rem can be used for the worker accident standard for unlikely events.

As can be seen in Table 2-1, a value of 25 rem/event is selected as the worker accident standard for both unlikely and extremely unlikely events. Because this is over 10 rem for the 10^{-2} to 10^{-4} probability range, satisfaction of the worker accident risk goal needs to be demonstrated.

For the RPP-WTP, this goal is satisfied by calculating the risk of facility operation to the workers. This is a best estimate analysis based on realistic input and modeling assumptions. In performing this analysis, all structures, systems, and components capable of preventing or mitigating the event are considered. Estimates of system and component unavailabilities and unreliabilities consider failure to start and failure to run as well as maintenance-caused unavailabilities. Accident prevention and mitigation features are added to the design as necessary to satisfy the worker accident risk goal. Note 2 of Table 2-1 explicitly commits the RPP-WTP contractor to this risk evaluation process.

The accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to an average individual in the vicinity of the Contractor's facility, of prompt fatalities that might result from an accident should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed." The DOE guidance document states that a radiation exposure standard of 100 rem/event would satisfy the accident risk goal. Because the RPP-WTP standard is 25 rem/event, the guidance document is satisfied.

In each of the four cells addressing accident exposure standards for workers and collocated workers in the unlikely and extremely unlikely events ranges, an ALARA accident limit is not specified. However, Note 3 of Table 2-1 states:

> "In addition to meeting the listed dose standards for accidents, the approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below standards to account for uncertainties in the analysis, and to provide for sufficient design margin and operational flexibility."

This approach provides an adequate level of safety. The following paragraphs should also be noted in support of this conclusion.

The accident analyses will show compliance with exposure standards for accidents. In addition, a defense-in-depth approach provides multiple levels of protection that ensure worker exposures from accidents will be significantly lower than calculated. This is a proven approach, considered to be effective at minimizing exposures to workers.

The approach to accident mitigation (as described in Note 3 of Table 2-1) is to examine accident consequences to ensure that calculated exposures are far enough below standards to account for uncertainties in the analysis and to provide sufficient design margin and operational flexibility. This approach is employed for all accidents (including both public and workers at all accident frequency levels) that can challenge the exposure standards, ensuring that accident exposures would be well below standards.

3.0 Development of the BNI Approach to Compliance with Table 1 of DOE/RL-96-0006

The overall approach to complying with DOE Table 1 is presented in this document. This approach takes the form of Table 2-1. The "To be derived" cells have been completed as discussed. The remaining cells of Table 2-1 are either identical or conservative with respect to DOE Table 1. The following sections discuss differences between DOE Table 1 and Table 2-1.

DOE Table 1 footnotes are not shown in Table 2-1. Section 2.1 of DOE/RL-96-0006 states that the footnotes refer only to the origin of the specific standards and, as such, are not considered contractual requirements unless included elsewhere in the contract.

3.1 Estimated Frequency of Occurrence

The second column of DOE Table 1, "Estimated Probability of Occurrence (P) (yr^{-1})," has been titled in Table 2-1, "Estimated Frequency of Occurrence (f) (yr^{-1})". In addition, the estimated frequency of occurrence for normal events of DOE Table 1 is redefined in Table 2-1 as any normal event regardless of frequency (nominally taken to be a frequency > 0.1/yr). The estimated frequency of anticipated events in DOE Table 1 is redefined as events with an annual frequency of occurrence of $10^{-2} < f\ 10^{-1}$.

With these changes, events routinely performed (e.g., melter replacement) are considered normal events rather than accidents, irrespective of frequency of occurrence. As normal events, the radiological assessment is subject to the more restrictive "per year" exposure standards rather than "per event" exposure standards. Consequently, these changes are conservative in comparison to DOE Table 1.

3.2 Normal Events/Public and Workers Exposure Standards

Clarifying descriptions have been included in the Normal Events/Public cell of Table 2-1 explaining that the second 100 mrem/yr standard applies to a member of the public entering the controlled area and the 25 mrem/yr standard is the public primary exposure standard for radioactive waste. The removal of DOE Table 1 footnotes (as noted above) necessitated the addition of these clarifying notes.

For the Normal Events/Worker and Normal Events/Collocated Worker cells of Table 2-1, the DOE Table 1 standard of 1.0 rem/yr ALARA design limit is replaced by a standard of 1.0 rem/yr ALARA design objective per 10 CFR 835, Section 1002(b). The corresponding worker standards for normal events in DOE Table 1 are tied to the ALARA design objectives of 10 CFR 835.1002(b) by the footnotes to DOE Table 1.

BNI has committed to full compliance with 10 CFR 835 in the SRD, and the other sections of 10 CFR 835.1002 provide adequate requirements to ensure routine worker exposures will be ALARA. In addition, a footnote, Note 1, is included in Table 2-1. This note states the following:

> "In addition to meeting the listed design objective of 10 CFR 835.1002(b), the inhalation of radioactive material by workers and collocated workers under normal conditions is kept ALARA through the control of airborne radioactivity as described in 10 CFR 835.1002(c)."

3.3 Anticipated Events/Worker and Collocated Worker Exposure Standards

References to as low as reasonably achievable (ALARA) standards have been removed for the Anticipated Events/Worker and Collocated Worker cells of Table 2-1. The ALARA design objective of 10 CFR 835, "Occupational Radiation Protection", is applied to normal events as shown in Table 2-1. However, with the redefinition in Table 2-1 of anticipated events as those events with an annual frequency of occurrence of $10^{-2} < f \leq 10^{-1}$, the ALARA objective no longer applies because anticipated events are not part of normal operation.

This change complies fully with Section 3.2, "Radiation Protection Objective", of DOE/RL-96-0006, which states the following:

> "Ensure that during normal operation radiation exposure within the facility and radiation exposure and environmental impact due to any release of radioactive material from the facility is kept as low as is reasonably achievable (ALARA) and within prescribed limits, and ensure mitigation of the extent of radiation exposure and environmental impact due to accidents."

This aspect of Table 2-1 also represents compliance with contractual requirements because footnote 3 of DOE Table 1 references 10 CFR 835.1002(b). This section, and 10 CFR 835.202 which it references, establishes design requirements for occupational exposures other than planned special exposures and emergency exposures. Administrative limits for planned special exposures and emergency exposures are addressed in 10 CFR 835.204 and 10 CFR 835.1302 and are complied with by the RPP-WTP.

Finally, to provide an adequate level of safety and to ensure that cost-effective safeguards affecting anticipated events are evaluated (and incorporated as appropriate) whenever the final calculated event consequence to a worker or collocated worker is 1 rem or more, the approach specifies a 1.0-rem/event design action threshold standard. In addition, a note is included in Table 2-1 to explain the application of the standard. This note (Note 4 to Table 2-1) states:

> "When a calculated accident exposure exceeds this threshold, then appropriate actions are taken. These include carrying out a less bounding (i.e., more realistic) evaluation to show that the accident consequences will be below the threshold or evaluating additional safeguards for cost-effectiveness and/or feasibility. This threshold is not a limit; it does not require the implementation of additional preventative or mitigative features if they are not both cost-effective and feasible."

3.4 Extremely Unlikely Events/Public Exposure Standard

A standard is included in the Extremely Unlikely Events/Public cell of Table 2-1 stating that a public exposure standard target value of 5 rem/event is applied to extremely unlikely events. This target value is based on the following:

- The philosophy is that the public should be protected by a lower exposure standard than a worker. This philosophy recognizes the fact that the worker has agreed to work on the Hanford Site and has received training for avoiding hazards and dealing with hazardous situations.
- A goal to facilitate transition to the NRC as the regulatory agency with jurisdiction over nuclear safety for DOE facilities. With the exception of a 25 rem/event guideline value of 10 CFR 100 for the establishment of the exclusion area and low population zone for commercial power reactors, the NRC has not established a public exposure standard that exceeds 5 rem/event. A public exposure standard of 5 rem/event is also included in proposed rulemaking for 10 CFR 70 (NRC 1995b), which further supports the Table 2-1 value.
- With the same 5 rem/event public exposure standard for both unlikely and extremely unlikely events, there is no need to bin accidents in one of these two event frequency categories for the purpose of establishing protection of public safety.

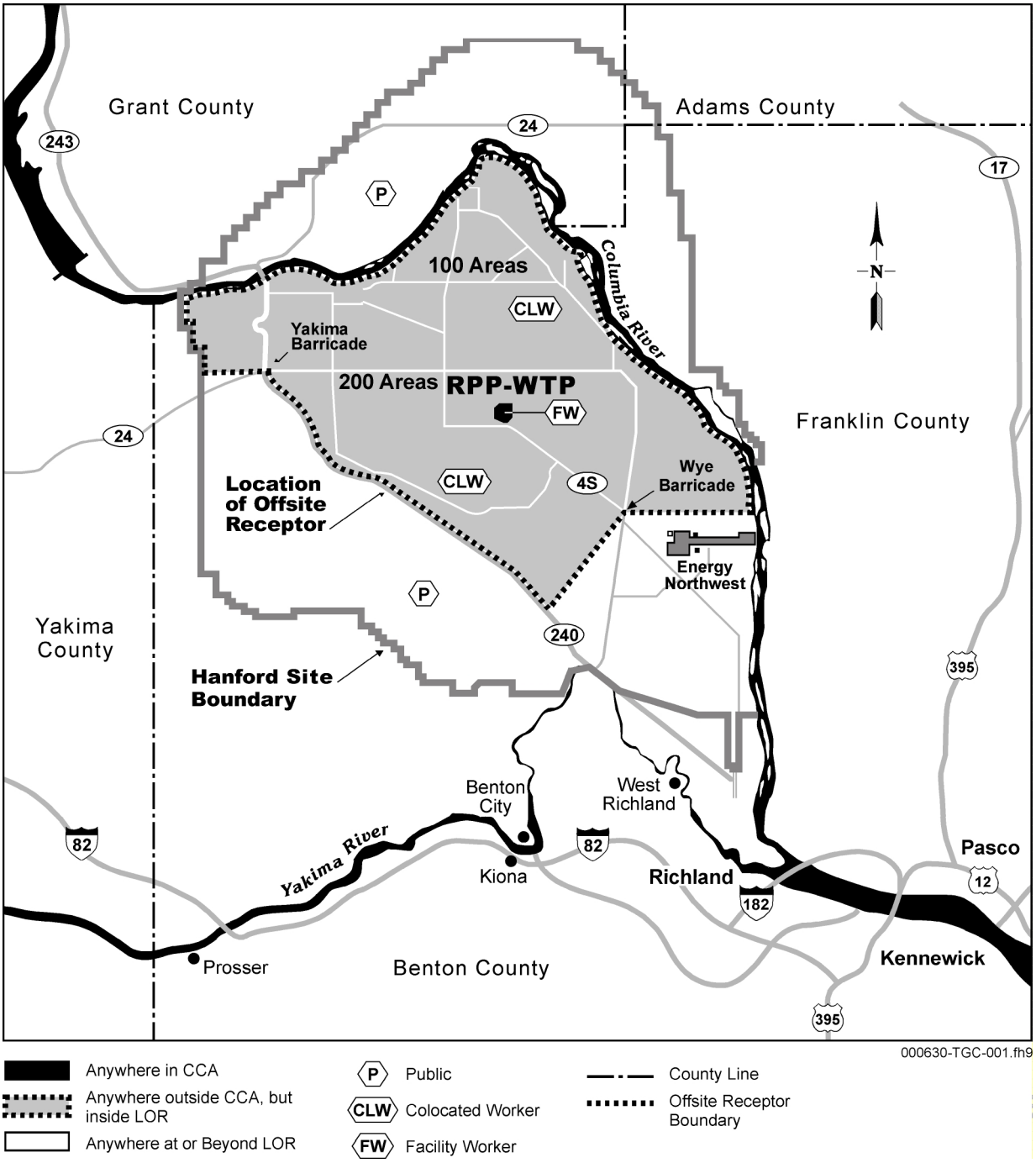
3.5 Location of Receptors

In Table 2-1, a new last row has been added to clarify in DOE Table 1 of DOE/RL-96-0006 the assumed location for the facility worker, the collocated worker, and the public, for the purpose of establishing compliance with the radiological standards of DOE Table 1. The bases for the receptor locations included in this row are provided below.

3.5.1 Facility Worker

The facility worker is located at the most limiting location within the RPP-WTP contractor-controlled area as defined in DOE/RL-96-0006, as shown in Figure D-1.

Figure D-1. Location of Facility and Collocated Workers.



Section 6.0, "Glossary", of DOE/RL-96-0006 defines the controlled area as the following:

> "The physical area enclosing the facility by a common perimeter (security fence). Access to this area can be controlled by the Contractor. The controlled area may include identified restricted areas."

The controlled area for RPP-WTP used to define the location of the facility worker, is that land within the RPP-WTP security fence.

3.5.2 Collocated Worker

Section 6.0, "Glossary", of DOE/RL-96-0006 defines the collocated worker as the following:

> "An individual within the Hanford Site, beyond the Contractor-controlled area, performing work for or in conjunction with DOE or utilizing other Hanford Site facilities."

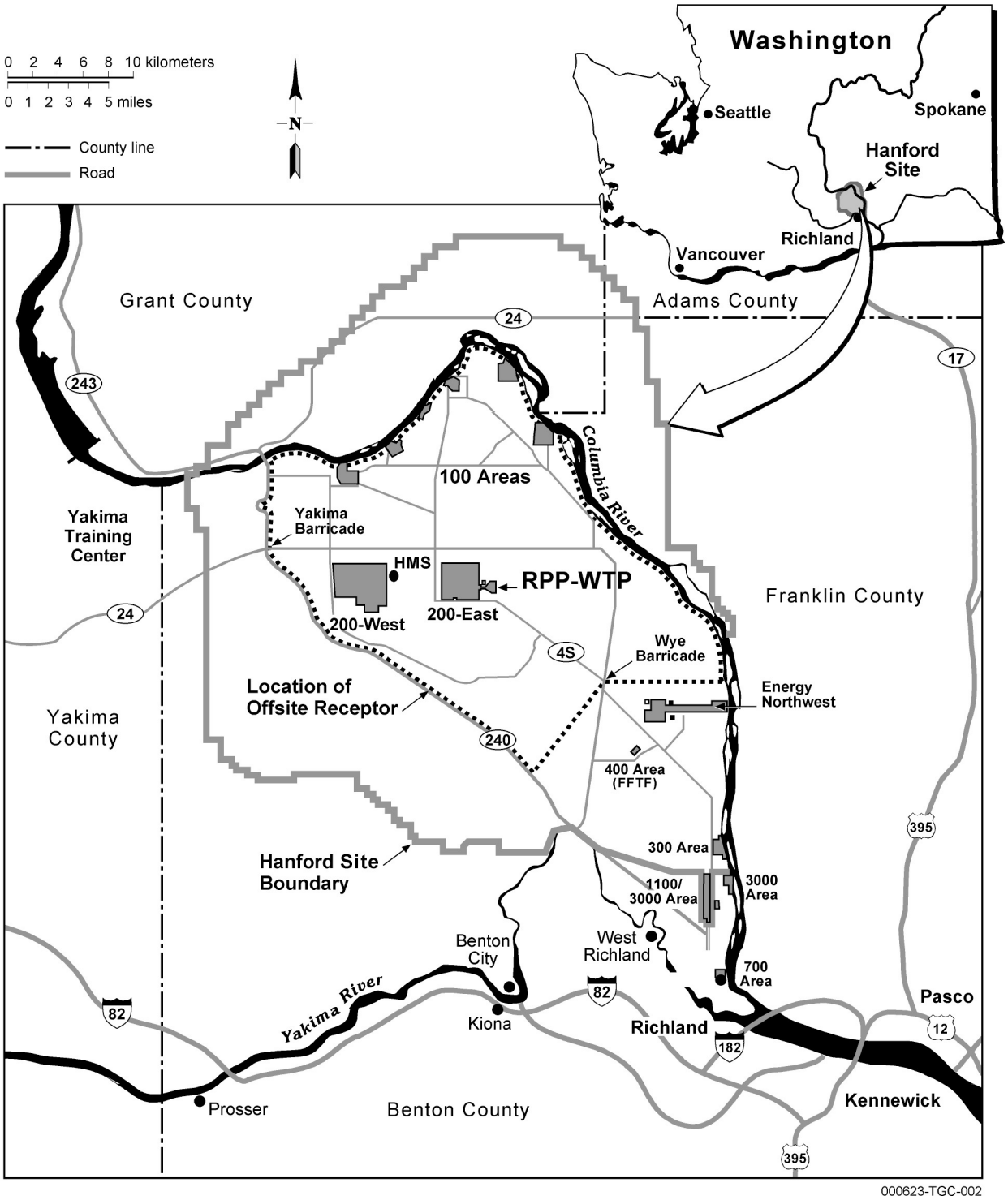
For evaluation of the RPP-WTP design to the exposure standards of DOE Table 1, the location of the collocated worker is either at the controlled area boundary or beyond that boundary if such a location results in higher exposure. For a ground-level release, the location of the collocated worker is considered no closer than 100 m from the release point.

3.5.3 Public

The location of the public (i.e., the offsite receptor) for the purpose of establishing compliance with the last column of DOE Table 1 of DOE/RL-96-0006, is established at the most limiting exposure location along the near bank of the Columbia River, Highway 240, and a southern boundary as shown in Figure D-2.

This area includes land for which it is reasonable to assume DOE will retain the right to control activities and limit access under accident conditions for the operating life of the RPP-WTP. Specifying the near river bank excludes the Columbia River for which DOE does not control activities (DOE-RL 1995). Specifying Highway 240 excludes the Arid Lands Ecology Reserve of which DOE might relinquish control during the operating life of the RPP-WTP. The southern boundary serves to exclude Energy Northwest's Columbia Generating Station, a commercial nuclear power plant (whose workers should be considered members of the public), and the Hanford Site 300, 400, and 1100 Areas. The 400 Area includes the Fast-Flux Test Facility.

Figure D-2. Boundary for Location of Offsite Receptor for the Purpose of Implementing DOE/RL-96-0006, Rev. 0, Table 1, Public Exposure Standard.



In footnotes 10 and 12, DOE Table 1 of DOE/RL-96-0006 makes reference to 10 CFR 72, "Licensing Requirements for the Independent Spent Fuel (ISFSI) and High Level Radioactive Waste," and 10 CFR 100, "Reactor Site Criteria," to relate to the public exposure standards for unlikely and extremely unlikely events. While the siting requirements and guidance of Parts 72 and 100 are not applicable to the RPP-WTP, the requirements for establishing the location of the offsite receptor in these two cited regulations are useful for locating the offsite receptor for a waste processing facility such as RPP-WTP. Section 72.106, "Controlled Area Boundary of an ISFSI or Monitored Retrievable Storage (MRS)", includes the following statements relative to the boundary to be assumed for the evaluation of radiological exposure to the public:

> "The minimum distance from the spent fuel or high-level radioactive waste handling and storage facilities to the nearest boundary of the controlled area shall be at least 100 meters."
>
> "The controlled area may be traversed by a highway, railroad or waterway, so long as appropriate and effective arrangements are made to control traffic and to protect public health and safety."

Title 10 CFR 100 establishes a guideline value of 25 rem for 2 hr at the exclusion area boundary. For the exclusion area, 10 CFR 100.3, "Definitions", states the following:

> "(a) *Exclusion area* means that area surrounding the reactor, in which the reactor licensee has the authority to determine all activities including exclusion or removal of personnel and property from the area. This area may be traversed by a highway, railroad, or waterway, provided these are not so close to the facility as to interfere with normal operations of the facility and provided appropriate and effective arrangements are made to control traffic on the highway, railroad, or waterway, in case of emergency, to protect the public health and safety. Residence within the exclusion area shall normally be prohibited. In any event, residents shall be subject to ready removal in case of necessity. Activities unrelated to operation of the reactor may be permitted in an exclusion area under appropriate limitations, provided that no significant hazards to the public health and safety will result."

As can be seen from the above excerpts, the assumed location for the offsite receptor for RPP-WTP is consistent with 10 CFR 72 and 10 CFR 100. In addition, the proposed southern boundary takes advantage of the road junction at the Wye barricade (Figure F-1) for control of access to the site during accident conditions.

4.0 References

10 CFR 70, "Domestic Licensing of Special Nuclear Material", *Code of Federal Regulations*, as amended

10 CFR 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-Level Radioactive Waste", *Code of Federal Regulations*, as amended

10 CFR 100, "Reactor Site Criteria", *Code of Federal Regulations*, as amended

10 CFR 835, "Subpart C - Standards for Internal and External Exposure", *Code of Federal Regulations*, as amended

AIChE, 1992, *Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York

DOE 1994, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, DOE-STD-3009-94, U.S. Department of Energy, Washington, D.C.

DOE 1995, *Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria*, DOE G 420.1-X, Revision G, U.S. Department of Energy, Washington, D.C.

DOE-RL 1995, *Clarification of Hanford Site Boundaries for Current and Future Use in Safety Analysis*, letter Walter B. Scott, DOE-RL to Contractors, dated September 26, 1995, U.S. Department of Energy, Richland Operations Office, Richland, Washington

DOE-RL 1996, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 0, U.S. Department of Energy, Richland Operations Office, Richland Washington

DOE-RL 1997, *Guidance for Review of TWRS Privatization Contractor Radiation Exposure Standards for Workers*, DOE/RL-97-09, U.S. Department of Energy, Richland Operations Office, Richland Washington

EPA 1991, *Manual of Protective Action Guides and Protective Actions for Nuclear Incidents*, U.S. Environmental Protection Agency, Washington, D.C.

NCRP 1963, *Maximum Permissible Body Burdens and Maximum Permissible Concentrations of Radionuclides in Air and in Water for Occupational Exposure*, Handbook 69, Addendum 1, National Bureau of Standards, Washington, D.C.

NRC 1995a, *Integrated Safety Analysis Guidance Document*, NUREG-1513, Draft, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC 1995b, *Preliminary Working Draft of Revision of 10 CFR 70 Updated*, 4/05/95, provided at the NRC public meeting of May 2, 1995, U.S. Nuclear Regulatory Commission, Washington, D.C.

Appendix E

Reliability, Availability, Maintainability, and Inspectability (RAMI)

To ensure that the facility meets operational requirements, it is necessary to address issues associated with reliability, availability, maintainability, and inspectability.

Reliability is used as a measure of the ability of an item or system to complete a task, and it is normally expressed as a probability of failure. Reliability is designed in through the use of appropriate design techniques and control of the mode of operation and the environment. Design techniques to be used vary because they are dependent on the specific item or system and the task to be performed. Their purpose is to optimize reliability by the following:

1) Use of proven materials and components
2) Design simplicity
3) Testability
4) Control of manufacturing standards
5) Control of operational mode (e.g., prevention of misuse and overloads)
6) Control of environment (e.g., protection against corrosion and vibration)

Consistent with the RPP-WTP process for tailoring hazard controls using the potential radiological and chemical consequences of individual events, reliability is assigned to SSCs based upon the importance of the SSC to the prevention or mitigation of accidents. The significance of accident prevention and mitigation is determined by the severity of the accident to workers or the public. To implement this tailoring in a clear, consistent, and defensible manner, an Implementing Standard for Safety Standards and Requirements Identification was developed. This Implementing Standard includes a Severity Level ranking system which provides the hazard assessment and control teams with a defined way to categorize the potential severity of those events that can result in radiological or hazardous exposure to the workers or the public. The Implementing Standard provides the means by which the hazard assessment and control teams establish target reliabilities for SSCs.

Availability is a measure of the degree to which an item or system is in an operable condition. It is expressed quantitatively as the ratio of the mean time between failures to the sum of the mean time between failures and the mean time to repair. System availability is calculated to determine the potential for downtime. In this way, systems are identified that contribute to decreased availability. Required availability is achieved by specifying additional systems or increasing reliability of existing systems.

Maintainability is a measure of the ability to restore a failed item or system to an operable condition in a specified time. Maintainability is designed into the facility and processes through use of appropriate design techniques, (e.g., the use of specially designed, remotely removable, and replaceable pumps and valves in process systems, and the placement of active pumps or valves within shielded accessible areas equipped with appropriate decontamination facilities that allow hands-on maintenance activities) and logistic support (e.g., scheduling and procedures). Benefits of these design techniques are that they simplify maintenance operations in high radiation areas and remove high maintenance equipment from high radiation areas. Testability of Safety Design Class systems and components is facilitated by such features as redundancy that allow for a system or component to be removed from service for maintenance or testing without loss of safety protection.

Inspectability is the measure of the ease with which items or systems can be inspected for preventative maintenance or assessment of condition. Inspectability is used to monitor facility items in order to maintain their reliability. Inspectability of facility items can be designed in by the use of shielded access areas (as above, to reduce radiation exposure) for active equipment or the provision of monitoring equipment (e.g., material coupons for determining vessel corrosion rates, and in-cell cameras).

During the design phase, the RPP-WTP facility and processes are evaluated for reliability, availability, maintainability, and inspectability. A number of validated modeling techniques (computer codes, mathematical modeling, failure modes, and effects analysis) for determining reliability and availability of the facility and processes are used. These are used to identify those facility and process areas that are sensitive with respect to influencing overall facility and process performance. Optimum reliability is established by the use of appropriate standards and quality control. The determination of maintenance and inspection needs is based on facility and process reliability requirements. It is a mixture of process optimization, provision of appropriate design features to aid preventative and scheduled maintenance and inspection, and the development of maintenance and inspection programs (administrative and procedural controls) whose objectives among other things, are to facilitate these activities. Reliability targets are assigned to SSCs only when a quantitative value has been credited for the reliability of an SSC in safety analysis.

Appendix F

Ad Hoc Implementing Standard for Deactivation and Decommissioning Planning

CONTENTS

Section **Page**

1.0 Introduction F-1
2.0 Plan Preparation F-1
3.0 Summary F-2
4.0 Definitions F-2

1.0 Introduction

All elements of the RPP-WTP safety approach are applied to the deactivation phase of the project. In addition, the RPP-WTP will incorporate design provisions to facilitate deactivation and final decommissioning as described in the implementing standard DOE G 441.1-2, *Occupational ALARA Program Guide*, for SRD Criterion 8.0 - 2. These provisions will reduce radiation exposure to Hanford Site personnel and the public during and following deactivation and decommissioning activities and minimize the quantity of radioactive waste generated during deactivation. The purpose of this standard is to define the attributes that must be addressed during the preparation of the deactivation plan to protect both the Hanford Site personnel and the public both during and after the deactivation stage of the project.

2.0 Plan Preparation

A deactivation plan will be prepared prior to construction of the RPP-WTP. The deactivation plan will provide details on how the following activities will be accomplished to achieve a deactivated status for the facility.

1) Verification of the completion of the facility deactivation end point. The term facility deactivation end point refers to the set of conditions that comprise the completion of facility deactivation i.e., radiological, structural, equipment, and documentation. These general end points will be defined in the deactivation plan and a requirement made to determine specific end points. When these end point criteria are met the facility will be in a safe state that can be economically monitored and maintained until final decommissioning.
2) Documentation of the regulatory status, conditions, and inventories of remaining radioactive and hazardous materials and health and safety requirements. After facility construction but before deactivation commences, the deactivation plan will require a hazard evaluation for radiological, nuclear, and process safety be carried out. Safety standards and requirements will be identified to implement the controls to protect against the facility hazards.
3) Identification of the facilities, structures, support systems, and surveillance systems to provide for confinement and monitoring of the remaining contamination, radiation, and other potential hazards. After facility construction but before deactivation commences, the plan will be expanded to describe the activities required to maintain the operability of critical equipment and to maintain the structural integrity of the deactivated facility. It will identify modification requirements to systems for the above purposes.
4) Posting and securing of the facility. After facility construction but before deactivation commences, the plan will be expanded to identify the radiological controls required for the deactivated facility, which will include posting of radiological areas. The need for other safety postings will also be identified.

5) Removal of packaged special nuclear materials and other packaged radiological and chemical materials.
6) Confirmation that security systems and procedures are adequate and in place to prevent unauthorized entry.
7) Waste minimization during the deactivation process.

3.0 Summary

The above requirements for the deactivation plan in combination with measures taken at the design stage of the project will protect the Hanford Site personnel and the public both during and following the deactivation activities.

4.0 Definitions

Deactivation - Placing the facility in stable and known conditions, identifying hazards, eliminating or mitigating hazards, and transferring programmatic and financial responsibilities from the operating program to the disposition program. Surveillance and maintenance continues to assure public, environment, and worker safety. The facility is in a safe storage mode, with ongoing, low levels of surveillance and maintenance. The general intent is that the facility be unoccupied and locked except for periodic inspections. Radioactive and hazardous materials may remain in the facility and are subject to ongoing regulatory oversight. (DOE/EM-0318, *Facility Deactivation Guide -- Methods and Practices Handbook*, December 1996)

Decommissioning - The process of removing a facility from operation, followed by decontamination, entombment, dismantlement, or conversion to another use. (DOE G 430.1-1A, *Life Cycle Asset Management*)

Decontamination - The reduction or removal of contaminating radioactive material from a structure, area, object or person. Decontamination may be accomplished by (1) treating the surface to remove or decrease the contamination, (2) letting the material stand so that the radioactivity is decreased as a result of natural decay, and (3) covering the contamination to shield or attenuate the radiation emitted. (Health Physics and Radiation Health Handbook, Revised Edition, Bernard Shleien, 1992)

End Point - Specifying and achieving end points is a systematic, engineering way of proceeding from an existing condition to a stated desired final set of conditions in which the facility is safe and can be economically monitored and maintained. (DOE/EM-0318, *Facility Deactivation Guide - Methods and Practices Handbook*, December 1996)

Appendix G

Ad Hoc Implementing Standard for Safety Analysis Reports

CONTENTS

1.0 Introduction G-1
2.0 Definitions G-1
3.0 Process G-1
    3.1 Safety Analysis Report Preparation G-1
4.0 References G-25

1.0 Introduction

The purpose of this Implementing Standard is to define the format and content for RPP-WTP safety analysis reports (SARs).

Section 2.0 provides the definitions important to this Implementing Standard. Section 3.0 defines the process for development, review, and approval.

2.0 Definitions

For the definitions of the following terms, see the reference provided.

Safety Analysis Report (SAR) (DOE/RL-96-0006 [DOE-RL 1998b])

3.0 Process

3.1 Safety Analysis Report Preparation

The River Protection Project Waste Treatment Plant (RPP-WTP) SARs document the safety analyses for the facility to demonstrate that it can be safety operated, maintained, and shut down.

The SARs shall be prepared in accordance with the requirements of:

1) DOE/RL-96-0003, *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors* (DOE-RL 1998a), Sections 4.3.2 and 4.3.3, both titled "Contractor Input"
2) Contract Table S7-1, "Radiological, Nuclear, and Process Safety Deliverables"
3) *Safety Requirements Document Volume II* (SRD) (BNI 2001), Safety Criterion 9.1-2

The content of the Preliminary Safety Analysis Report (PSAR) and the Final Safety Analysis Report (FSAR) are developed using the guidance provided in the Nuclear Regulatory Commission's 1995 draft revision to Regulatory Guide 3.52, *Standard Format and Content for Heatlh and Safety Sections of License Applications for Fuel Cycle Facilities* (NRC 1995). The content of the SARs is tailored to the nature of the RPP-WTP relative to the hazards and hazardous situations identified by the process hazards analysis. Planned deviations from the content guidance of draft Regulatory Guide 3.52 are identified in Table G-1.

The Table of Contents for the safety analysis reports follows Table G-1. The safety analysis report will not be submitted to the regulator until all major safety issues have been resolved and other safety issues have been scheduled for completion. The FSAR should identify significant changes made in the facility design and plans for operation from what was presented in the PSAR. The FSAR, in addition to including facility and process drawings, should also include fabrication and construction specifications important to the safety analysis of the facility.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
1.3 Site Description	Regulatory Guide (RG 3.52) suggests that Section 1.3 summarize information used in preparing the Environmental Report. Specific information is referenced, but not duplicated in the safety analysis report (SAR).	The Environmental Report provides this information.
1.3.2 Demography and Land Use	The population distribution as a function of distance and direction is not to be provided. The distances to nearby population centers are provided.	There are no residences on the Hanford Site and the nearby population is low.
3.3 Quality Assurance	Section 3.3.4, "Quality Assurance Program Description" addresses the 10 criteria of 10 CFR 830 Subpart A, "Quality Assurance Requirements" in lieu of the 18 criteria listed in RG 3.52.	By contract compliance to the 10 CFR 800 series of nuclear safety requirements is required. This includes compliance to 10 CFR 830 Subpart A, "Quality Assurance Requirements". The differences in the criteria to be addressed are not significant because the quality assurance programs are based on consensus standards.
3.5 Human Factors	RG 3.52 states that a formal human factors program is not required if the facility has no requirement for safety-class actions. Human factors are considered in the Preliminary Safety Analysis Report (PSAR) independent of whether or not human actions are required for protection of the public or workers.	The requirements of DOE/RL-96-0006 (DOE-RL 1998a), Section 4.2.6, "Human Factors", extend beyond consideration of human factors as related to actions taken to protect the public. Final Safety Analysis Report (FSAR) Section 3.5 documents how compliance to contract Section 4.2.6 is achieved.
3.10 Testing Program and Preoperational Safety Review	This section is added to address the initial and commissioning testing programs.	Addition of this section facilitates documentation of compliance to DOE/RL-96-0006 (DOE-RL 1998b), Section 4.2.8, "Pre-Operational Testing", and Section 5.2.6, "Pre-Startup Safety Review", and DOE/RL-96-0003 (DOE-RL 1998a), Section 4.3.2, "Contractor Input", item 13.
3.11 Operational Practices	This section is to added to address such conduct of operations considerations as shift routine and turnover, control area activities, communications, control of on-shift training, control of equipment and system status, lockout and tagout, independent verification of equipment status, logkeeping, and operational aids postings.	These items are discussed to address what is normally considered conduct of operations.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
4.7 Results of the Integrated Safety Assessment	The results for unmitigated accidents are compared to the radiological standards discussed in Integrated Safety Management Plan (ISMP) Section 1.2, "Detailed Description of the Safety Approach" rather than to 10 CFR 20, "Standards for Protection Against Radiation". A full assessment of the hazardous situations that might present themselves during facility operation is provided. This includes estimates of radiological and chemical releases for this range of events. Additional details are provided on the methodology used for consequence analysis, bounding conditions, input assumptions, and accident sequences.	The standards provided in RG 3.52 were derived from 10 CFR 20, "Standards for Protection Against Radiation", which is applicable to normal operation. The nature of the accidents for the RPP-WTP requires more discussion of consequence analysis than that required of fuel fabrication facilities.
4.8 Controls for Prevention and Mitigation of Accidents	This section identifies the specific safeguards selected for protection of the facility workers, as well as safeguards selected for protection of the public and collocated workers.	The nature of the accidents for the RPP-WTP requires more discussion of consequence analysis than that required for fuel fabrication facilities.
5.0 Radiation Safety	Chapter 5.0 provides the upper-level statutory standards and program policies that ensure the radiological safety of employees, visitors, and onsite members of the public. Deviations from RG 3.52 are as follows: 1) As an U.S. Nuclear Regulatory Commission (NRC) document, RG 3.52 references and specifies applicable portions of 10 CFR 20. Because 10 CFR 835 is the radiation safety regulation for the RPP-WTP, the focus of this section is on 10 CFR 835. 2) The implementation-level standards and guidance documents referenced in RG 3.52 is being incorporated into the Radiation Protection Plan (RPP).	Compliance with 10 CFR 835 is a requirement of the contract. The RPP required by 10 CFR 835 is required to include some of the information required of RG 3.52. There is no need to present this information in two documents.
5.1 As Low As Reasonably Achievable (ALARA) Policy and Program	RG 3.52 states that Regulatory Guide 8.10, Revision 1R (*Operating Philosophy for Maintaining Occupational Radiation Exposures As Low As Reasonably Achievable)* should be used in the development of the ALARA program. DOE guidance such as DOE G 441.1-2, *Occupational ALARA Program Guide* will also be used to develop the RPP-WTP ALARA program for normal operation.	DOE practices have proven to be successful for facilities similar to the RPP-WTP.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
5.3 Radiological Safety Standards	Section 5.3 is added to provide the radiation standards by which the program operates. The standards specifically identify regulatory exposure standards, administrative exposure control levels, and other key standards of the radiation protection program.	The contract requires compliance to the 10 CFR 800 series of nuclear safety requirements. This includes compliance to 10 CFR 835, "Occupational Radiation Protection". Section 5.3 documents the compliance to the exposure standards of those regulations that have been promulgated.
5.8 External Exposure (renumbered 5.9 from RG 3.52)	By RG 3.52, the applicant is expected to participated in the National Voluntary Laboratory Accreditation Program (NVLAP) external dosimetry. Section 5.8 allows for participation in either the NVLAP or U.S. Department of Energy (DOE) Laboratory Accreditation Program (DOELAP) accreditation programs.	The option of participating in either the NVLAP or the DOELAP provides maximum flexibility and equivalent dosimetry program quality
5.14 Radioactive Waste Management	RG 3.52 does not require a discussion of waste management systems.	Section 5.14 is added to the SARs as the Process Hazards Analysis (PHA) completed for the RPP-WTP have identified hazards and hazardous situations with the waste management features of the facility. It is a requirement of DOE/RL-96-0003 (DOE-RL 1998a), Section 4.1.2, "Contractor Input", that deliverables be tailored to the nature and level of hazards associated with its waste processing activities.
Appendix 5A Radiation Protection Program Outline	This appendix is added to address compliance to 10 CFR 835.	The contract requires compliance to the 10 CFR 800 series of nuclear safety requirements. This includes compliance to 10 CFR 835, "Occupational Radiation Protection".
Appendix 5B Environmental Radiation Protection Program Outline	This appendix is added to address compliance to the requirements of the Environmental Protection Agency (EPA) and Washington State laws and regulations.	The contract requires submittal of an outline for the environmental radiological protection plan.
Chapter 6.0 Nuclear Criticality Safety	The methodology for criticality analyses is provided in the SARs to the extent the need to perform criticality calculation is found to be appropriate. The RPP-WTP SARs provide fewer details and commitments compared to fuel fabrication facilities relative to: 1) Nuclear criticality safety organization (Section 6.2.1) 2) Criticality training (Section 6.2.5) 3) Specific maintenance and quality assurance provisions for criticality prevention (Sections 6.2.3 and 6.2.4) 4) Audits and inspection (Section 6.2.6)	RG 3.52 focuses heavily on accidental criticality which is a more significant concern for fuel fabrication facilities which have a much higher inventory and concentrations of fissile material than the RPP-WTP. See ISMP Section 3.8, "Criticality Safety", for additional information.

Table G-1 Deviations from the Safety Analysis Report Content Guidance of Regulatory Guide 3.52 [1]

Chapters	Addition or Subtraction	Basis
7.4 "Hazardous Waste Management"	Section 7.4 of the RPP-WTP SARs address all chemical inventories that are identified by the PHA as representing a significant hazard.	By Section 4.2.2, "Contractor Input", of DOE/RL-96-0003 (DOE-RL 1998a), the Initial Safety Analysis Report (ISAR) is to address process safety as well as radiological and nuclear safety. The need to address all aspects of chemical safety is also a NRC requirement of RG 3.52, Section 7.4, and NUREG-1513, "Integrated Safety Analysis Guidance Document", (draft) (NRC 1994). The NUREG-1513 definition of "integrated" provided in Section 2.1, "Definition", makes reference to chemical safety. Specific guidance for chemical safety is provided in Section 2.6.2, "Process Safety Information", of the NUREG-1513.
10.0 Environmental Protection	This chapter references the Environmental Report	Protection of the environment is addressed in a separate document.
11.0 Deactivation and Decommissioning	This chapter addresses design and operational provisions considered to facilitate deactivation and decommissioning. It does not address the financial considerations for decommissioning.	The scope of the contract (DOE-ORP 2000) is limited to design support for deactivation.

1. Standard Format and Content for the Health and Safety Sections of License Applications for Fuel Cycle Facilities, Regulatory Guide 3.52, Revision 2, draft, U.S. Nuclear Regulatory Commission, Washington D.C. (NRC 1995).

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
1.1.1 Facility Description	A description of the facility design is provided in sufficient detail to demonstrate the facility design and construction requirements of the Safety Requirements Document (SRD). The details are also sufficient to support an understanding of the safety analysis provided in section 4.2, "Facility Description".	This section updates the general description of the facility design.
1.1.2 Process Description	This section describes the process design in sufficient detail to demonstrate the system and component design and fabrication requirements of the SRD are satisfied. Details on the process design sufficient to support an understanding of the safety analysis are provided in section 4.3, "Process Description".	This section updates the general description of the process design.
1.2 Institutional Information	This section provides the information required by RG 3.52, draft (NRC 1995a).	This section updates any changes in the institutional information provided in the PSAR.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
1.3 Site Description	A description of the site land use, meteorology, hydrology, geology, and seismology is provided.	This section address any existing or planned changes in land use from that provided in the PSAR. The FSAR provides any new meteorology, hydrology, geology, and seismology data made available. However, the level of detail provided for these subject areas is not significantly different between the two SARs. The FSAR summarizes data obtained during the Facility excavation that confirms the adequacy of the design. This includes the results of field and laboratory investigation of soil properties.
2.1 Organization and Administration	The Project organizational charts with a focus on the design and construction management organizations are provided. An organization chart for the operational phase is also presented. More definitive information on the roles, responsibilities, and interfaces for project management, engineering, construction management, inspections, procurement, quality assurance, records management, and nuclear safety functions is included. Section 2.1 also provides the criteria to determine minimum staffing requirements. A summary of procedures to be developed to implement the regulatory requirements addressed in this section is presented.	The section contains an update to the organizational structure of Project with a focus on operational and operational support organizations. This section also includes: 1 Title of each position that is important to public and worker safety and reporting relationship 2 Description defining qualifications, responsibilities, and authorities for each position related to safety 3 Organizational charts of the line organization and safety organization 4 Title of the individual delegated overall responsibility for the safety programs who has the authority to shut down operations if they appear to be unsafe, including independence of this authority from operational constraints 5 Lines of responsibility and authority for safety 6 Lines of communication and interfaces between organizations inside the facility 7 Availability of personnel within the safety organization to carry out the assigned function Specific information on procedure development and minimum staffing requirements is provided.
2.2 Safety Committees	Information on responsibilities, authorities, and proposed charters of safety committees, and oversight groups is provided.	This section updates information on safety committees, and oversight groups that are established following issuance of the PSAR and addresses any new safety committees that have been established.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.1 Configuration Management	This section contains specific information on: 1 Content and reference to procedures used to maintain effective configuration management of the RPP-WTP 2 Scope of identified systems, structures, and components (SSCs) and their relationship to the contents of Chapter 4.0, "Integrated Safety Analysis" 3 Description of the design information package contents to be provided to the safety analysts 4 Change control system specifics, including identification, technical and management reviews, documentation, and implementation 5 Specific physical configuration assessment, and periodic equipment performance monitoring 6 Design, installation, and testing of facility modifications 7 Revision of operating, test, calibration, surveillance, and maintenance procedures and drawings 8 Selection and control of replacement parts 9 Description of how the RPP-WTP design requirements and design basis were established and documented A summary of procedures developed to implement the regulatory requirements addressed in this section 3.1 is presented. This section also includes a draft of the unreviewed safety question process.	Specific information on the content of procedures and training developed is provided. The final unreviewed safety question process is provided.
3.2 Maintenance	A list of Safety Design Class and Safety Design Significant SSCs is provided. The maintenance implementation plan is described to such a level that maintenance philosophy and approach are evident.	The FSAR may modify the list of SSCs actions to be addressed based on safety analysis of the final design. Specific information on procedures and training developed to implement the requirements of section 3.2 is provided. In addition, the elements of the finalized maintenance implementation plan is described. Also discussed is the application of information obtained from demonstration testing and commissioning programs to the maintenance program (the latter by FSAR amendment after initial submittal).

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.3 Quality Assurance	Information related to the roles, responsibilities, and interfaces for project management, engineering, construction management, inspections, procurement, quality assurance, records management, and nuclear and process safety functions is provided. Included is the organizational structures of the quality assurance organization. The PSAR describes the quality assurance requirements of SSCs. Requirements for procedures to implement the regulatory requirements is presented.	For the FSAR, this section focuses on the quality assurance program for the operating RPP-WTP. Specific information on procedures and training developed to implement the requirements of section 3.3 is provided.
3.4 Training and Qualification	A description of the performance-based training program for operational and support personnel, including a detailed description of the training development process, is provided. The administrative process to be applied to training activities is described to a level such that the elements of the program and management's commitment to training is evident.	Details on the training and qualification program are provided. Also discussed is the application of information obtained from demonstration testing and commissioning programs (the latter by FSAR amendment after initial submittal).
3.5 Human Factors	This section documents the criteria by which human factors are considered in the facility design and operation.	This section states how human error in facility operations was taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions. Consideration given in the design to detecting and correcting or compensating for errors is discussed.
3.6 Audits and Assessments	Information on the performance of audits and assessments is incorporated into this section.	This section is focused on audits and assessments performed during RPP-WTP operation. Specific information on procedures and training developed to implement the requirements of this section is provided.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.7 Incident Investigation	This section includes the following: 1 Provisions for establishing investigating teams 2 Functions, responsibilities, and scope of authority of investigating teams 3 Qualifications of internal and/or external investigators on investigating teams 4 A description of the procedures to ensure prompt investigation of an incident 5 Policy directives that the investigative process and the investigating team be independent of line management and that participants be assured of no retribution from participating in investigations 6 The approach proposed to determine the root cause(s) of incidents to ensure that the process is reasonable, systematic, and structured 7 Methods to ensure that corrective actions to resolve findings from incident investigations are tracked to completion 8 Identification and application of lessons learned 9 Specific reporting criteria for incident reporting during the construction phase. A summary of procedures developed to implement the regulatory requirements addressed in section 3.7 is presented.	Specific information on procedures and training developed to implement the requirements is provided. Included are specific reporting criteria for incident reporting during the operations phase.
3.8 Records Management	This section contains the organization structure and a description of the records management system, including authorities, responsibilities, and qualifications of personnel managing Environmental, Safety, and Health (ES&H) records. A summary of procedures developed to implement the regulatory requirements contained in section 3.8 is presented.	Specific information on procedures and training developed to implement the requirements is provided.
3.9 Procedures	A description of the administrative controls to ensure that work is performed in accordance with established technical standards and using approved instructions and procedures is provided.	This section describes the detailed processes of selecting activities requiring operating, emergency, and support procedures; preparing procedures; verifying and validating procedures; and reviewing and approving procedures. In addition, the program to administratively control procedures and their use is described in detail.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
3.10 Testing Program and Preoperational Safety Review	This section describes the analysis used to identify and define pre-operational and commissioning tests and describes tests required to ensure compliance to safety specifications. The testing program and controls are described to a level such that the testing philosophy and approach are evident. The prestart safety review approach is described to a level such that the areas to be evaluated and the evaluation approach are evident.	This section may modify the list of required safety improvement program and commissioning tests based on safety analysis of the final design. In addition, the administrative and program controls applicable to the test program are described in full.
3.11 Operational Practices	A description is provided of operational practices influenced by design details (i.e., communications systems, operational hazards associated with systems and hardware, and control area arrangements).	A description is provided of the operational practices influenced by the final design. In addition, final descriptions are provided on controls and administration of operational practices.
4.0 Integrated Safety Analysis	The methodology for hazards identification and accident analyses is described. The accident consequence analyses include margins in assumptions, boundary conditions, modeling and comparisons to acceptance criteria, as appropriate, to account for uncertainties in the design and plans for operation. Section 4.7 addresses the relationship of these uncertainties to the need to provide sufficient information in the construction authorization package to allow for issuance of the construction authorization.	Assumption used the PSAR to account for uncertainties in the design and plans for operations are removed from the FSAR analysis to the extent that these uncertainties have been resolved.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.2 Facility Description	In addition to providing a general description of the facility, this section discusses the basic civil/structural criteria to be applied to the design. For those structures classified as Safety Design Class, this includes the following: 1 Design codes, standards, and specifications 2 Loading criteria and load combinations 3 Design and analysis methodology 4 Structural acceptance criteria 5 Criteria for identifying testing and in-service inspection requirements 6 Material specifications 7 Special construction features This section also discusses: 1 Assumed soil properties 2 Excavation, backfill, and recompaction criteria 3 Assumed bearing capacity of the soil and the safety factor applied to this capacity 4 Expected static and dynamic building total and differential settlements. Less detail is provided for Safety Design Significant structures. Section 4.2 gives specific attention to those structures classified in Section 4.8 as Safety Design Class. Structures located away from the buildings containing significant hazards and that have no relationship to nuclear or process safety are briefly described (e.g., structural design, and the contents and functions of the building) and identified on a plot plan.	The FSAR updates the facility description and basic civil/structural criteria provided in the PSAR. It follows with discussions of the results of the application of these criteria to specific features of the facility. Examples are as follows: 1 The confirmation of soil properties obtained during excavation 2 A table providing the building total and differential settlement data obtained 3 Derived soil damping values 4 The results of the soil/structure analysis 5 Developed floor response spectra and time histories 6 A list of moderate and high energy systems 7 A list of specific missile and jet impingement sources, targets, and barriers provided. Also provided are updated plan and section drawings for structures classified as Important-to-Safety. These drawings show the basic floor arrangements, location of major systems and equipment, and basic building dimensions. For those structures classified as Safety Design Class, the drawings also show key structural elements, such as panel and floor reinforcements, cell liners, leak chases, major equipment anchors, and the use of masonry walls.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.3 Process Description	The description of process systems includes process flow diagrams for the major systems with instrumentation, sample points, and control features noted to the extent they have been developed. Heat loads are provided for heat transfer systems important to the safety analysis. Design features and parameters important to Section 4.7, "Results of the Integrated Safety Assessment", are provided. This section contains the following additional detail for each system classified as Safety Design Class: 1 The specified safety function(s) with reference to PSAR Section 4.7 for the basis 2 The design basis to be applied in the development of the system design 3 Design margins to be applied 4 The criteria to be used for the development of material specifications 5 Criteria to be used to determine design limits (such as pressure and temperature) 6 Criteria to be used to identify the need for instrumentation to monitor process conditions and the design criteria for such instrumentation (e.g., application of the single-failure criterion, and testability). For many cases, the design criteria provided are those included in the SRD.	This section updates the PSAR description of process systems. Process and instrumentation diagrams are provided for major systems. In addition, for those systems classified as Safety Design Class, the FSAR describes how the design requirements provided in the PSAR are reflected in the final design. For each system classified as Safety Design Class, the following are provided: 1 The specified safety function(s) with reference to Section 4.7 for the basis 2 The design basis 3 The design safety margins provided by the final design 4 Important quantitative design parameters met by the system design with their basis (e.g., heating, ventilation, and air-conditioning flow, and what established the minimum and maximum flow limits) 5 Material specifications 6 Established design limits and their basis (e.g., maximum pressure and temperature limits and what established these limits) 7 Instrumentation provided with attributes, including redundancy, diversity, in situ testability, environmental qualification, failure mode on loss of power, and the surveillance requirements as defined in section 4.8, "Controls for Prevention and Mitigation of Accidents". The means by which the monitoring requirements established in section 4.8 are also to be discussed in the FSAR. Potential adverse system interactions between systems of various design classification are addressed.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
4.7 Results of the Integrated Safety Analysis (ISA)	In addition to providing the results of the Process Hazards Analysis (PHA) and accident analysis, this section discusses the uncertainties of the PHA and accident analysis and relates these uncertainties to the required content of the construction authorization package. Section 4.7 provides the basis for the conclusion that resolution of the uncertainties will not have a significant impact on the construction authorization request. This discussion includes the following: 1 Characterization of the specific technical information that must be obtained to demonstrate acceptable resolution of the uncertainties 2 An outline and schedule of the program to resolve uncertainties 3 A discussion of the design and/or operational alternatives to resolve the uncertainties Section 4.7 of the PSAR also describes the preliminary Fire Hazard Analysis (FHA) and the consequence of each design-basis fire scenario, including the consequences in the area of origin and adjacent areas.	This section documents the resolution of any uncertainties identified in the PSAR. The FSAR describes the final FHA and all resolved uncertainties previously included in the PSAR and additional fire protection measures and equipment design.
4.8 Controls for Prevention and Mitigation of Accidents	Draft Technical Safety Requirements are included.	Final Technical Safety Requirements are included.
5.0 Radiation Safety	This chapter identifies the radiological exposure standards by which the radiation safety program is developed and the facility is operated to ensure the radiological safety of the public and workers. This chapter identifies the radiation protection criteria to be implemented in the facility design.	This chapter reflects the final facility design developed to the radiation protection criteria. It also describes the facility organization and plans for the conduct of operations. This chapter includes detail on facility operation within the radiological protection program exposure standards and other radiological protection requirements.
6.0 Criticality	The methodology for criticality analyses is provided to the extent the need to perform criticality calculation is found to be appropriate. The analyses may include margins in assumptions, bounding conditions, modeling and comparisons to the acceptance criterion, as appropriate, to account for uncertainties in the design and plans for operation.	Assumptions used in the PSAR to account for uncertainties in the design and plans for operations are removed from the FSAR criticality analysis to the extent that these uncertainties have been resolved. The FSAR describes the remaining criticality controls appropriate for the RPP-WTP.
7.0 Chemical Safety	The chapter identifies the program standards by which the chemical safety program is developed and operated to protect the public and workers against chemical hazards and hazardous situations. This chapter identifies criteria to be used for the development of chemical safety controls.	The chapter reflects the final facility design and facility organization and the developed plans for conduct of operations as related to chemical safety. This section also identifies the specific chemical safety controls to be implemented for protection of the public and workers.

Table G-2 Planned Differences Between Regulatory Guide 3.52 PSAR and FSAR Content [1]

Title	PSAR	FSAR
8.0 Fire Safety	This chapter describes automatic and manual fire protection features and administrative controls of the fire safety program. Also described are features of the ventilation system, building layout, and emergency egress routes important to fire safety.	Administrative controls to be implemented for the fire safety program are described, including final responsibilities of response forces, and the pre-fire plan used by firefighting personnel to suppress fires safely and effectively.
9.0 Emergency Management	This chapter identifies the applicable requirements and criteria to which the RPP-WTP Emergency Management Program are developed. A general outline of the program is presented and the relationship to the Hanford Site and local emergency management programs is discussed. Information is presented to demonstrate that the RPP-WTP staff will be able to attain an acceptable state of emergency preparedness by the time the facility becomes operational.	The FSAR discusses and references the specific emergency plan and implementing documentation prepared for the RPP-WTP. Specific aspects of all elements of the emergency preparedness program are discussed. Information is presented demonstrating the developed emergency preparedness program is compliant with applicable requirements, regulations, criteria, and guidance, and capable of responding to any operational emergency at the facility.
10.0 Environmental Protection	This chapter references the RPP-WTP Environmental Report submitted in Part A.	This chapter references the RPP-WTP Environmental Report as a new or revised Environmental Report and is not required to support the operating authorization request.
11.0 Deactivation and Decommissioning	This chapter identifies design considerations given to facilitate deactivation and decommissioning. It also discusses in general terms the planning, safety analysis, and regulatory considerations to be given to deactivation.	The chapter describes the specific design features included to facilitate deactivation and decommissioning. The level of detail for planning, safety analysis, and regulatory considerations to be given to deactivation is about the same as that provided in the PSAR. The FSAR is amended near the end of waste processing operation to provide more specific information regarding deactivation. (See Integrated Safety Management Plan Table 9-5.)

[1] *Standard Format and Content for the Health and Safety Sections of License Applications for Fuel Cycle Facilities*, Regulatory Guide 3.52, Revision 2, draft, US Nuclear Regulatory Commission, Washington, DC (NRC 1995).

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
	Introduction		Executive Summary
1.0	General Information	N/A	
1.1	Facility and Process Description		Executive Summary
1.1.1	Facility Description	2.3 2.4	Facility Overview Facility Structures
1.1.2	Process Description	2.5	Process Description
1.2	Institutional Information	N/A	
1.2.1	Identity and Address	1.1	Introduction
1.2.2	Activity	N/A	
1.2.3	Site Location	1.3.1	Geography

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
1.2.4	Type, Quantity, and Form of Licensed Material	3.3.2	Hazard Identification (Vol II - V)
1.3	Site Description	1.3	Site Description
1.3.1	Geography	1.3.1	Geography
1.3.2	Demography and Land Use	1.3.2	Demography and Land Use
1.3.3	Meteorology	1.4.1	Meteorology
1.3.4	Hydrology	1.4.2	Hydrology
1.3.5	Geology and Seismicity	1.4.3	Geology
2.0	Management Organization	17	Management, Organization, and Institutional Safety Provisions
2.1	Organization and Administration	17.3	Organizational Structures, Responsibilities, and Interfaces
2.1.1	Organizational Commitments, Relationships, Responsibilities, and Authorities	17.3	Organizational Structures, Responsibilities, and Interfaces
2.1.2	Management Controls	17.4	Safety Management Policies and Programs
2.2	Safety Committees	17.4.2	Safety Review and Performance Assessments
3.0	Conduct of Operations	11	Operational Safety
3.1	Configuration Management	17.4.3	Configuration Management
3.2	Maintenance	10.5	Maintenance
3.3	Quality Assurance	14	Quality Assurance
3.3.1	Management Commitment for QA Program	14	Quality Assurance
3.3.2	Scope of QA Program	14	Quality Assurance
3.3.3	Organizational Responsibility	14	Quality Assurance
3.3.4	QA Program Description	14	Quality Assurance
3.3.5	Graded QA Approach	14	Quality Assurance
3.3.6	Application of Graded QA to SSCs and Activities	14	Quality Assurance
3.4	Training and Qualification	12	Procedures and Training
3.4.1	Organization and Management of the Training System	12.4	Training Program
3.4.2	Trainee Selection	12.4	Training Program
3.4.3	Conduct of Needs/Job Analysis and Identification of Tasks	12.4	Training Program
3.4.4	Development of Learning Objectives as the Basis for Training	12.4	Training Program

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
3.4.5	Organization of Instruction Using Lesson Plans and Other Training Guides	12.4	Training Program
3.4.6	Evaluation of Trainee Mastery of Learning Objectives	12.4	Training Program
3.4.7	Conduct of On-The-Job Training	12.4	Training Program
3.4.8	Systematic Evaluation of Training Effectiveness	12.4	Training Program
3.5	Human Factors	13	Human Factors
3.5.1	Organization and Administration	13.3	Scope of Human Factors Process
3.5.2	Human Factors and Assessment of the Correction of Deficiencies	13.4	Human Factors Program
3.6	Audits and Assessments	17.4.2	Safety Review and Performance Assessment
3.7	Incident Investigations	13.4	Human Factors Program
3.8	Records Management	17.4.4	Document Control and Records Management
3.8.1	Organization and Administration	17.4.4	Document Control and Records Management
3.8.2	Types of Records	17.4.4	Document Control and Records Management
3.8.3	Record Handling Procedures	17.4.4	Document Control and Records Management
3.8.4	Record Storage and Protection	17.4.4	Document Control and Records Management
3.9	Procedures	12.3	Procedures Program
3.10	Testing Program and Preoperational Safety Review	10.3	Commissioning
3.11	Operational Practices	11.3	Conduct of Operations
4.0	Integrated Safety Analysis	3	Hazard and Accident Analysis
4.1	Site Description	1.3	Site Description
4.2	Facility Description	2.3 2.4	Facility Overview Facility Structures
4.3	Process Description	2.5	Process Description
4.4	Process Safety Information	3.3.3.X	Hazard Evaluation
4.5	Training and Qualifications of ISA Team	3.3.1	Identification of Work
4.6	ISA Methods	3.X	Hazard and Accident Analysis
4.7	Results of the Integrated Safety Assessment	3.3.3 (Vol II - V)	Development of Control Strategies

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
4.8	Controls for Prevention and Mitigation of Accidents	3.4 (Vol II - V)	Accident Analysis Methodology
4.9	Administrative Control of the ISA		Executive Summary
5.0	Radiation Safety	7	Radiation Protection
5.1	As Low As Reasonably Achievable (ALARA) Policy	7.1	Introduction
5.2	Organizational Relationships and Personnel Qualifications	7.1	Introduction
5.3	Radiological Safety Procedures and Radiological Work Permits (RWPs)	7.1	Introduction
5.4	Training	7.1	Introduction
5.5	Ventilation systems	2.6	Confinement Systems
5.6	Air Sampling	7.1	Introduction
5.7	Contamination Control	7.1	Introduction
5.8	External Exposure	7.1	Introduction
5.9	Internal Exposure	7.1	Introduction
5.10	Summing Internal and External Exposure	7.1	Introduction
5.11	Respiratory Protection	7.1	Introduction
5.12	Instrumentation	7.1	Introduction
5.13	Integrated Safety Analysis	3.4	Accident Analysis Methodology
5.14	Radioactive Waste Management	8	Hazardous Material Protection
6.0	Nuclear Criticality Safety	6	Criticality Safety Program
6.1	NCS Technical Practices	6.3 6.4	Criticality Limits and Concerns Criticality Controls
6.1.1	Process Analysis from the Integrated Safety Analysis	6.4.6	Application of Double Contingency Principle
6.1.2	NCS Evaluations	6.4.6	Application of Double Contingency Principle
6.1.3	NCS Limits	6.4.3	Administrative Controls
6.1.4	Validation and Use of Analytical Methods	6.4.4	Methodology for Determining Criticality Limits
6.1.5	NCS Control Methods	6.4.3	Administrative Controls
6.1.6	Criticality Accident Alarm System	6.6	Criticality Instrumentation
6.2	Administrative Practices	6.5	Criticality Protection Program
6.2.1	NCS Organizational Responsibilities	6.5	Criticality Protection Program
6.2.2	Configuration Management	17.4.3.2	Configuration Management Process
6.2.3	Maintenance	6.4.3	Administrative Controls

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
6.2.4	Quality Assurance (QA)	6.4.3	Administrative Controls
6.2.5	Training	6.5.4	Criticality Safety Training and Qualifications
6.2.6	Operational Inspections, Audits, Assessments, and Investigations	6.5.5	Criticality Safety Training and Qualifications
6.2.7	Written Operating Procedures	6.5.3	Administrative Controls
6.2.8	Materials Control for NCS	N/A	
6.2.9	Emergency Preparedness	6.6	Criticality Instrumentation
7.0	Chemical Safety	8	Hazardous Material Protection
7.1	Chemical Safety Responsibility	8.3	Hazardous Material Protection and Organization
7.2	Chemical Safety Approach	8.6	Hazardous Material Exposure Control
7.3	Chemical Safety Controls	8.6	Hazardous Material Exposure Control
7.4	Hazardous Waste Management	8.6	Hazardous Material Exposure Control
8.0	Fire Safety	N/A	
8.1	Organization and Conduct of Operations	18.3	Organization and Management
8.1.1	Organization and Management	18.3	Organization and Management
8.1.2	Training and Qualifications	18.4	Training and Qualifications
8.1.3	Fire Prevention Program	18.5	Fire Prevention Program
8.2	Fire Protection Features and Systems	18.6	Fire Protection Features and Systems
8.3	Manual Fire-Fighting Capability	18.7	Manual Fire-Fighting Capability
8.4	Fire Hazard Analysis	18.8	Fire Hazard Analysis
8.5	References	N/A	
9.0	Emergency Management	15	Emergency Preparedness
9.1	Description of On-Site and Off-Site Emergency Facilities	15.4.4	Emergency Facilities and Equipment
9.2	Types of Accidents	3.3.3	Development of Control Strategies
9.3	Classification of Accidents	3.3.3	Development of Control Strategies
9.4	Detection of Accidents	15.4	Emergency Preparedness Planning
9.5	Mitigation of Consequences	15.4	Emergency Preparedness Planning
9.6	Assessment of Releases	15.4	Emergency Preparedness Planning
9.7	Responsibilities of Licensee and Other Organizational Personnel	15.4	Emergency Preparedness Planning
9.8	Notification and Coordination	15.4	Emergency Preparedness Planning
9.9	Description of the Emergency Operational Center	15.4	Emergency Preparedness Planning

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
9.10	Information to be Communicated and the Parties to be Contacted	15.4	Emergency Preparedness Planning
9.11	Public Notification	15.4	Emergency Preparedness Planning
9.12	Training	15.4	Emergency Preparedness Planning
9.13	Procedures for Safe Shutdown and Recovery	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
9.14	Drills and Exercises	15.4	Emergency Preparedness Planning
9.15	Procedures for Identifying, Locating, and Controlling Hazardous Chemicals	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
9.16	Responsibilities for Developing and Maintaining Current the Emergency Program and Its Procedures	15.3 15.4	Scope of Emergency Preparedness Program Emergency Preparedness Planning
10.0	Environmental Protection	9.1	Introduction
10.1	Environmental Report	N/A	
10.1.1	Description of Proposed Action	N/A	
10.1.2	Purpose of Proposed Action	N/A	
10.1.3	Description of Affected Environment	N/A	
10.1.4	Discussion of Considerations	N/A	
10.1.5	Analysis of Environmental Effects of Proposed Action and Alternatives	N/A	
10.1.6	Federal and State Environmental Requirements	9.1.1 9.4	Permit Overview Radioactive and Hazardous Waste Processes
10.2	Environmental Safety Program	9.3	Radioactive and Hazardous Waste Management Program and Organization
10.2.1	Features for Contamination Control	2.3	Facility Overview
10.2.2	Environmental Monitoring Program	9.1 9.4	Introduction Radioactive and Hazardous Waste Processes
10.2.3	Emergency Plan	15.X	
10.2.4	Maintenance and Surveillance	9.3	Radioactive and Hazardous Waste Management Program and Organization
10.2.5	Configuration Management	17.4.3.2	Configuration Management Process
10.2.6	Organization and Management	9.3.1 17	Program Summary Management, Organization, and Institutional Safety Provisions
10.2.7	Quality Assurance	14.1	Introduction

Table G-3 Regulatory Guide 3.52 vs SAR Table of Contents Crosswalk

RG 3.52 Chapter		WTP New Location	
Section	**Title**	**Section**	**Title**
10.2.8	Training	9.3 9.7 (ERPP)	Radioactive and Hazardous Waste Management Program and Organization Environmental Radiological Protection Plan (ERPP)
10.2.9	Event Notification and Reporting	9.1.1	Permit Overview
10.2.10	Bibliography	9.8	References
11.0	Decommissioining	16	Deactivation and Decommissioning
11.1	Conceptual Decommissioning Plan	16.1	Introduction
11.1.1	Information for Conceptual Decommissioning Plan	16.4	Deactivation Requirements
11.1.2	Information for Total or Partial Cessation of Operations	16.5	Transition Readiness
11.1.3	Bibliography	16.7	References
11.1.4	Appendix A: Cost Estimating Tables	N/A	
11.2	Decommissioning Funding Plan and Financial Assurance Mechanisms	N/A	
11.2.1	Decommissioning Cost Estimate	N/A	
11.2.2	Financial Assurance Mechanism(s)	N/A	
11.2.3	Updating the Cost Estimate and Funding Level	N/A	
11.2.4	Bibliography	N/A	
11.2.5	Appendix A: Sample Sight Draft	N/A	
Appendix A	Radiation Protection Program Outline	7 RPP	Radiation Protection
Appendix B	Environmental Radiation Protection Program Outline	9.5 ERPP	Environmental Radiation Protection Plan (ERPP)

The SARs should include multiple volumes. Volume I should provide information that is applicable to more than one of the facilities (e.g., Pretreatment, Low-Activity Waste Vitrification, High-Level Waste Vitrification, and Balance of Facilities). Other volumes should be facility specific and contain, at a minimum, chapters 2, 3, 4, and 5.

Executive Summary

- **E.1 Facility Background and Mission**
- **E.2 Facility Overview**
- **E.3 Facility Hazard Classification**
- **E.4 Safety Analysis Overview**
- **E.5 Organization**
- **E.6 Safety Analysis Conclusions**
- **E.7 SAR Organization**
- **E.8 Summary of Significant Changes from the Preliminary Safety Analysis Report (FSAR stage)**

1 Site Characteristics

- **1.1 Introduction**
- **1.2 Requirements**
- **1.3 Site Description**
- **1.4 Environmental Description**
- **1.5 Natural Phenomena Hazards**
- **1.6 External Man-Made Threats**
- **1.7 Nearby Facilities**
- **1.8 References**

2 Facility Description

- **2.1 Introduction**
- **2.2 Requirements**
- **2.3 Facility Overview**
- **2.4 Facility Structures**
- **2.5 Process Description**
- **2.6 Confinement Systems**
- **2.7 Safety Support Systems**
- **2.8 Utility Distribution Systems**
- **2.9 Auxilliary Systems and Support Facilities**
- **2.10 References**

3 Hazard and Accident Analyses
- **3.1 Introduction**
- **3.2 Requirements**
- **3.3 Hazard Analysis Methodology**
- **3.4 Accident Analysis Methodology**
- **3.5 Hazard Classification**
- **3.6 Common Cause and Common Mode Design Basis Events**
- **3.7 Seismic Probabilistic Risk Assessment**
- **3.8 Adherence to Risk Goals and Results**
- **3.9 References**

4 Important to Safety Structures, Systems, and Components
- **4.1 Introduction**
- **4.2 Requirements**
- **4.3 Safety Design Class Systems, Structures, and Components**
- **4.4 Safety Design Significant Systems, Structures, and Components**
- **4.5 References**

5 Derivation of Technical Safety Requirements
- **5.1 Introduction**
- **5.2 Requirements**
- **5.3 Technical Safety Requirement Coverage**
- **5.4 Derivation of Facility Modes**
- **5.5 Technical Safety Requirement Derivation**
- **5.6 Design Features**
- **5.7 Interface with TSRs from Other Facilities**
- **5.8 References**

6 Criticality Safety Program
- **6.1 Introduction**
- **6.2 Requirements**
- **6.3 Criticality Limits and Concerns**
- **6.4 Criticality Controls**
- **6.5 Criticality Protection Program**
- **6.6 Criticality Instrumentation**
- **6.7 References**

7 Radiation Protection
- **7.1 Introduction**
- **7.2 Requirements**
- **7.3 References**

8 Hazardous Material Protection
- **8.1 Introduction**
- **8.2 Requirements**
- **8.3 Hazardous Material Protection and Organization**
- **8.4 ALARA Policy and Program**
- **8.5 Hazardous Material Training**
- **8.6 Hazardous Material Exposure Control**
- **8.7 Hazardous Material Monitoring**
- **8.8 Hazardous Material Protection Instrumentation**
- **8.9 Hazardous Material Protection Record Keeping**
- **8.10 Hazard Communication Program**
- **8.11 Occupation Chemical Exposures**
- **8.12 References**

9 Waste Management
- **9.1 Introduction**
- **9.2 Requirements**
- **9.3 Radioactive and Hazardous Waste Management Program and Organization**
- **9.4 Radioactive and Hazardous Waste Processes**
- **9.5 Waste Sources and Characteristics**
- **9.6 Waste Handling or Treatment Systems**
- **9.7 Environmental Radiological Protection Plan**
- **9.8 References**

10 Initial Testing, In-Service Surveillance, and Maintenance
- **10.1 Introduction**
- **10.2 Requirements**
- **10.3 Commissioning**
- **10.4 Surveillance Program**
- **10.5 Maintenance**
- **10.6 References**

11 Operational Safety
- **11.1 Introduction**
- **11.2 Requirements**
- **11.3 Conduct of Operations**

12 Procedures and Training
- **12.1 Introduction**
- **12.2 Requirements**
- **12.3 Procedures Program**
- **12.4 Training Program**
- **12.5 References**

13 Human Factors
- **13.1 Introduction**
- **13.2 Requirements**
- **13.3 Scope of Human Factors Process**
- **13.4 Human Factors Programmatic Interactions**
- **13.5 Optimization of Human Factors Elements**
- **13.6 References**

14 Quality Assurance
- **14.1 Introduction**
- **14.2 Requirements**
- **14.3 References**

15 Emergency Preparedness
- **15.1 Introduction**
- **15.2 Requirements**
- **15.3 Scope of Emergency Preparedness Program**
- **15.4 Emergency Preparedness Planning**
- **15.5 References**

16 Deactivation and Decommissioning
- **16.1 Introduction**
- **16.2 Requirements**
- **16.3 Design and Operational Features**
- **16.4 Deactivation Requirements**
- **16.5 Transition Readiness**
- **16.6 Turning Over WTP Facilities to DOE**
- **16.7 References**

17 Management, Organization, and Institutional Safety Provisions
- **17.1 Introduction**
- **17.2 Requirements**
- **17.3 Organizational Structures, Responsibilities, and Interfaces**
- **17.4 Safety Management Policies and Programs**
- **17.5 References**

18 Fire Protection
- **18.1 Introduction**
- **18.2 Requirements**
- **18.3 Organization and Management**
- **18.4 Training and Qualification**
- **18.5 Fire Prevention Program**
- **18.6 Fire Protection Features and Systems**
- **18.7 Manual Fire-Fighting Capability**
- **18.8 Fire Hazard Analysis**
- **18.9 Fire Protection for Filter Plenums**

4.0 References

BNI, 2001. *Safety Requirements Document Volume II*, 24590-WTP-SRD-ESH-01-001-02. Bechtel National, Inc., Richland, Washington.

DOE-ORP, 2000. Contract No. DE-AC27-01RV14136, December 2000. US Department of Energy, Office of River Protection, Richland, Washington.

DOE-RL, 1998a. *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0003, Revision 1. US Department of Energy, Richland Operations Office, Richland, Washington.

DOE-RL, 1998b. *Top-Level Radiological, Nucelar, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 1. US Department of Energy, Richland Operations Office, Richland, Washington.

NRC, 1994. *Integrated Safety Analysis Guidance Document*, draft NUREG-1513, distributed 8 August 1994, US Nuclear Regulatory Commission, Washington, DC.

NRC, 1995. Regulatory Guide 3.52, *Standard Format and Content for the Heatlh and Safety Sections of License Applications for Fuel Cycle Facilities*, draft Revision 2, US Nuclear Regulatory Commission, Washington, DC.