

Regulatory Unit Position on the Achievement of Adequate Safety



September 28, 2000

Office of Safety Regulation of the RPP-WTP Contractor

U.S. Department of Energy
Richland Operations Office
P.O. Box 550, A4-70
Richland, Washington 99352

PREFACE

The U.S. Department of Energy's (DOE) Richland Operations Office (RL) issued the *TWRS Privatization Request for Proposal (RFP)* for Hanford Tank Waste Remediation System (TWRS) Privatization in February 1996. Offerors were requested to submit proposals for the initial processing of the tank waste at Hanford. Some of this radioactive waste has been stored in large underground storage tanks at the Hanford Site since 1944. Currently, approximately 54 million gallons of waste containing approximately 240,000 metric tons of processed chemicals and 250 mega-curies of radionuclides are being stored in 177 tanks. These caustic wastes are in the form of liquids, slurries, saltcakes, and sludges. The wastes stored in the tanks are defined as high-level radioactive waste (10 CFR Part 50, Appendix F) and hazardous waste (Resource Conservation and Recovery Act).

The contract concept was for DOE to enter into a fixed-price contract for the contractor to build and operate a facility to treat the waste according to DOE specifications. The TWRS Privatization Program was divided into two phases, Phase I and Phase II. Phase I was a proof-of-concept/commercial demonstration-scale effort the objectives of which were to (a) demonstrate the technical and business viability of using privatized contractors to treat Hanford tank waste; (b) define and maintain adequate levels of radiological, nuclear, and process safety; (c) maintain environmental protection and compliance; and (d) substantially reduce life-cycle costs and time required to treat the tank waste. The Phase I effort consisted of two parts: Part A and Part B.

Part A consisted of a twenty-month development period to establish appropriate and necessary technical, operational, regulatory, business, and financial elements. This included identification by the TWRS Privatization Contractors and approval by DOE of appropriate safety standards, formulation by the Contractors and approval by DOE of integrated safety management plans, and preparation by the Contractors and evaluation by DOE of initial safety assessments. Of the twenty-month period, sixteen months were used by the Contractors to develop the Part-A products and four months were used by DOE to evaluate the products.

Part B was to consist of a demonstration period to provide tank waste treatment services by the TWRS Privatization Contractors who successfully completed Part A. Demonstration was to address a range of wastes representative of those in the Hanford tanks. Part B was to be 10 to 14 years in duration. Within Part B, wastes were to be processed during a 5- to 9-year period resulting in treatment of 6 to 13 percent of the Hanford tank waste.

Phase II was to be a full-scale production phase in which the remaining tank waste would be processed on a schedule that would accomplish removal from all single-shelled tanks by the year 2018. The objectives of Phase II were to a) implement the lessons learned from Phase I; and b) process all tank waste into forms suitable for final disposal.

In May 2000, DOE chose to terminate the privatization contract and seek new bidders under a different contract strategy. The program name was also changed from the Tank Waste Remediation System to the River Protection Project (RPP). The RPP is under the direction of the Office of River Protection, which was created by Congress in 1998 to assume programmatic responsibility for the entire Tank Waste Remediation System, including the waste treatment plant (WTP).

A key element of the River Protection Project Waste Treatment Plant (RPP-WTP) is DOE regulation of safety through a specifically chartered, dedicated Regulatory Unit (RU) at RL. This regulation by the RU is authorized by the document entitled *Policy for Safety Regulation of the RPP-WTP Contractor* (referred to as the Policy) and implemented

through the document entitled *Memorandum of Agreement for the Execution of Safety Regulation of the RPP-WTP Contractor* (referred to as the MOA). The Under Secretary of Energy; the Assistant Secretary for Environment, Safety and Health (ASEH); and the Assistant Secretary for Environmental Management (ASEM) signed the Policy. The MOA is signed by the ASEH and the ASEM. The nature and characteristics of this regulation are also specified in these documents. The MOA details certain interactions among RL, the ASEH, and the ASEM as well as their respective roles and responsibilities for implementation of this regulation.

The authority of the RU to regulate the RPP-WTP Contractor is derived solely from the terms of the RPP-WTP Contract and for the interim design period, from DOE Memorandum from Huntoon to French, dated May 23, 2000. Its authority to regulate the Contractor on behalf of DOE is derived from the Policy. The nature and scope of this special regulation (in the sense that it is based on terms of a contract rather than formal regulations) is delineated in the MOA, the RPP-WTP Contract, and the documents, listed below, which are incorporated into the Contract. This special regulation by the RU in no way replaces any legally established external regulatory authority to regulate in accordance with duly promulgated regulations nor relieves the Contractor from any obligations to comply with such regulations or to be subject to the enforcement practices contained therein.

The Policy, the MOA, the RPP-WTP Contract, and the documents incorporated in the Contract define the essential elements of the regulatory program, which are being executed by the RU and to which the RPP-WTP Contractor must conform. The four radiological, nuclear and process safety-related documents incorporated in the Contract (and also incorporated in the MOA) are:

Concept of the DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor, DOE/RL-96-0005,

DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor, DOE/RL-96-0003,

Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for the RPP Waste Treatment Plant Contractor, DOE/RL-96-0006, and

Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Plant Contractor, DOE/RL-96-0004.

The non-radiological safety document is:

Industrial Hygiene and Safety Regulatory Plan, RL/REG-2000-04.

In the execution of the regulatory program, the RU considers not only the relevant approaches and practices of DOE but also those of the U.S. Nuclear Regulatory Commission (NRC) and the Occupational Safety and Health Administration (OSHA). The Policy states that

"It is DOE's policy that the RPP-WTP Contractor activities be regulated in a manner that assures adequate safety by application of regulatory concepts and principles consistent with those of the Nuclear Regulatory Commission and the Occupational Safety and Health Administration."

To this end, the RU interacts with the NRC and the OSHA during development and execution of its regulatory program.

All documents issued by the Office of Safety Regulation of the RPP-WTP Contractor are available to the public through the DOE/RL Public Reading Room at the Consolidated Information Center, Room 101L, Richland, Washington. Copies may be purchased for a duplication fee.

This page intentionally left blank.

Table of Contents

1.0	PURPOSE	1
2.0	BACKGROUND	1
3.0	DISCUSSION	7
3.1	Compliance with Laws and Regulations	8
3.2	Management System and Administrative Process Principles	9
	3.2.1 Quality Assurance	9
	3.2.2 Radiation Protection	10
	3.2.3 Training	11
	3.2.4 Facility Operation	12
	3.2.5 Emergency Planning	13
	3.2.6 Unreviewed Safety Question Determinations	14
	3.2.7 Authorization Basis	14
	3.2.8 Safety Responsibility/Culture/Oversight	15
	3.2.9 Process Safety Principles	16
3.3	Facility Design, Analysis, Construction, and Pre-Operational Testing Principles	17
	3.3.1. General Principles	18
	3.3.2 Principles Influencing Safety Requirements and Standards Selection	25
4.0	POSITION	36
5.0	REFERENCES	40
6.0	LIST OF TERMS	42

List of Figures

Figure 1. Adequate Safety Triad	4
Figure 2. Radiological and Nuclear Safety Principles	5
Figure 3. Top-Level Standards and Principles for Design, Construction, Pre-Operational Testing, Operation, and Safety Programs/Institutions	6

List of Tables

Table 1. Dose Standards Above Normal Background	21
Table 2. Accident Severity Level Identification	26
Table 3. Implementation of Defense-in-Depth by SSC	33

This page intentionally left blank.

REGULATORY UNIT POSITION ON THE ACHIEVEMENT OF ADEQUATE SAFETY

1.0 PURPOSE

This paper describes the position of the Office of Safety Regulation of the RPP-WTP Contractor (Regulatory Unit) on achieving adequate safety in the design and operation of the River Protection Project Waste Treatment Plant (RPP-WTP). Adequate safety is achieved by (1) applying the principles of integrated safety management which includes implementing the contractually prescribed process for requirements and standards selection, (2) complying with applicable laws and regulations, and (3) conforming to U.S. Department of Energy (DOE)-stipulated top-level standards and principles.

This paper was motivated in part by interactions between the Regulatory Unit (RU) and the Defense Nuclear Facilities Safety Board (DNFSB).^{1,2} The DNFSB interactions disclosed that the RU's position on the subject of adequate safety was insufficiently clear. It is intended that this paper will serve to communicate the RU thinking on the subject to a broad audience, especially the RPP-WTP Contractor.

2.0 BACKGROUND

DOE/RL-96-25, *Policy for Radiological, Nuclear, and Process Safety Regulation of the RPP-WTP Contractors* states that one of its objectives is to ensure that the activities of the RPP-WTP Contractor provide adequate safety through the following:

- Application of the principles of integrated safety management which includes implementing the contractually prescribed process for requirements and standards selection.
- Compliance with applicable laws and regulations.
- Conformance with DOE-stipulated top-level standards and principles.

The RPP-WTP Contract³ states⁴ in Standard 4, that “The primary objectives of the Safety, Health, and Environmental Program are to: ... implement a cost-effective program that integrates safety, health, and environmental protection in all Contractor activities.” Standard 4 goes on to state “The Contractor shall develop and implement an integrated standards-based safety management program to ensure that radiological, nuclear, and process safety requirements are defined,

¹ 00-RU-0091, *BNFL Developments in ISM*, Briefing by Clark Gibbs, December 9, 1999.

² 00-RU-0234, *Co-Located Worker Dose Limits*, Briefing by Clark Gibbs, February 15, 2000.

³ Contract No. DE-AC27-96RL13308, between DOE and BNFL Inc., dated September 24, 1998.

⁴ This contract has been terminated. It is expected that it will be replaced with a contract containing substantially similar language.

implemented, and maintained. Radiological, nuclear, and process safety requirements shall be adapted to the specific hazards that are identified with the Contractor's waste treatment services. The Contractor's integrated standards-based safety management program shall be developed to comply with the specific nuclear safety regulations defined under the 10 CFR 800 series of nuclear safety requirements and with the regulatory program established in DOE/RL-96-0003, *DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor*, DOE/RL-96-0004, *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Plant Contractor*, DOE/RL-96-0005, *Concept of the DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor*, and DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for the RPP Waste Treatment Plant Contractor*.

DOE/RL-96-0006 identifies the top-level standards and principles to which the design and operation of RPP-WTP must conform. DOE/RL-96-0004 specifies the process to be used by the RPP-WTP Contractor to establish safety standards and requirements within the framework of an integrated safety management program. DOE-RL-96-0003, describes the regulatory actions that the RU will take in the regulation of the RPP-WTP Contractor. The Standards Approval regulatory action⁵ described in DOE/RL-96-0003 specifies that RU approval of the Contractor's recommended set of radiological, nuclear, and process safety standards and requirements, as documented in the Contractor's Safety Requirements Document (SRD), is based on a determination that, if the selected standards and requirements are properly implemented, adequate safety will be achieved.

Taken together, the three elements of the Policy objectives described above are referred to as the "safety triad." The RU cannot make a favorable determination of adequate safety in the absence of any of the three elements. The adequate safety triad is shown in Figure 1. Included in Figure 1 is some description of the content of each of the three legs of the triad (i.e., compliance, conformance, and integrated safety management).

DOE/RL-96-0006 includes, among other things, the Radiological and Nuclear Safety Principles. Note that the Radiological and Nuclear Safety Principles are one component of the conformance leg as shown in Figure 1. Figure 2 displays the diversity and extent of the elements comprising the Radiological and Nuclear Safety Principles. This figure reveals the essential RPP-WTP approach to achieving adequate safety. Adequate safety is not achieved through one or two "silver bullets". The dose standards or the risk goals, discussed later in this paper, or even the standards-based integrated safety management process are not singly or collectively relied upon to achieve adequate safety. It is the combination of all the elements contained in the triad, integrated with appropriate attention to process safety, that is relied upon to achieve adequate safety on RPP-WTP. The basic principle is that if one requirement proves to have shortcomings, there are a host of others that mitigate any deficiencies in any one area. This approach results from the application of the principle of diversity and redundancy, a time-honored safety concept in nuclear facilities, to the fundamental safety requirements themselves.

⁵ DOE/RL-96-0003, Section 3.3.1.

Another way to visualize the safety approach is exemplified by Figure 3. Figure 3 represents the safety requirements for the physical facility as overlays of general design requirements, prescriptive design requirements, hazard and safety/accident analyses, and risk analyses. The requirements that are associated with the hazard and safety/accident analyses are the accident dose standards, and the requirements associated with the risk analyses are the risk goals. In turn, the physical facility requirements are supplemented by institutional arrangements requiring ALARA, control in normal range, etc.

The compliance leg of the safety triad identifies the laws and regulations applicable to the RPP-WTP. The RPP-WTP Contractor's integrated safety management (ISM) program must comply with these laws and regulations in the accomplishment of adequate safety in the design and operation of the RPP-WTP. A brief discussion of the laws and regulations applicable to RPP-WTP is provided in Section 3.1; however, compliance with applicable laws and regulations is not the emphasis of this position paper.

Considerable effort has been put forth by the RU in providing guidance to the RPP-WTP Contractor on standards-based, ISM. This includes the process for establishing a set of radiological, nuclear, and process safety standards and requirements (DOE/RL-96-0004) tailored to the work to be performed and its hazards, which the RPP-WTP Contractor is required by the Contract to follow. The RU has issued several position papers and a topic-specific study on the subject of standards-based ISM, as follows:

RL/REG-98-08, *Regulatory Unit Position on Selected Hazards Control Strategy Issues*, clarifies the RU's expectations for implementation of the required process for establishing safety standards and application of the top-level standards and principles. This paper was needed because the RPP-WTP Contractor made assumptions and identified standards in the Standards Approval and Initial Safety Assessment submittals that were not justified based upon the work identification and hazards evaluations contained therein.

RL/REG-98-13, *Standards Identification Exercise*, was prepared to demonstrate the execution of the Contract-stipulated standards selection process and to provide a detailed, informed basis for discussions with the RPP-WTP Contractor on RU expectations for Contractor execution of the standards identification process.

RL/REG-98-21, *Regulatory Unit Position on Implementing and Assuring Compliance with Integrated Safety Management*, shows how ISM is central to the RPP-WTP regulatory concept. The paper shows how ISM flows through the regulatory process, finally becoming embodied in the RPP-WTP Contractor's deliverables. The paper also describes the tools available to the RU to ensure compliance with the concepts of ISM.

RL/REG-99-16, *Regulatory Unit Position on the Selection of Design Standards*, discusses acceptable methods for selection of design standards by the RPP-WTP Contractor for the control of potential hazards. The RU position provided in this paper is that the Contractor should select and confirm standards using (1) engineering experience, (2) facility experience, (3) safety specifics, (4) costs, (5) contract requirements, (6) legal requirements, and (7) reliability associated with prior use of the standard.

RL/REG-99-18, *Regulatory Unit Position on Assessment of the Contractor's Integrated Safety Management Program as Described in the Integrated Safety Management Plan*, describes the RU's intentions for performing comprehensive assessments of the RPP-WTP Contractor's ISMP implementation. This paper also describes how the RU's oversight of the Contractor's ISM program compares with the DOE-wide oversight of contractors' ISM systems and RU plans for evaluating the impact of DOE-wide changes in ISM implementation on the Contractor's ISM program.

Figure 1. Adequate Safety Triad.

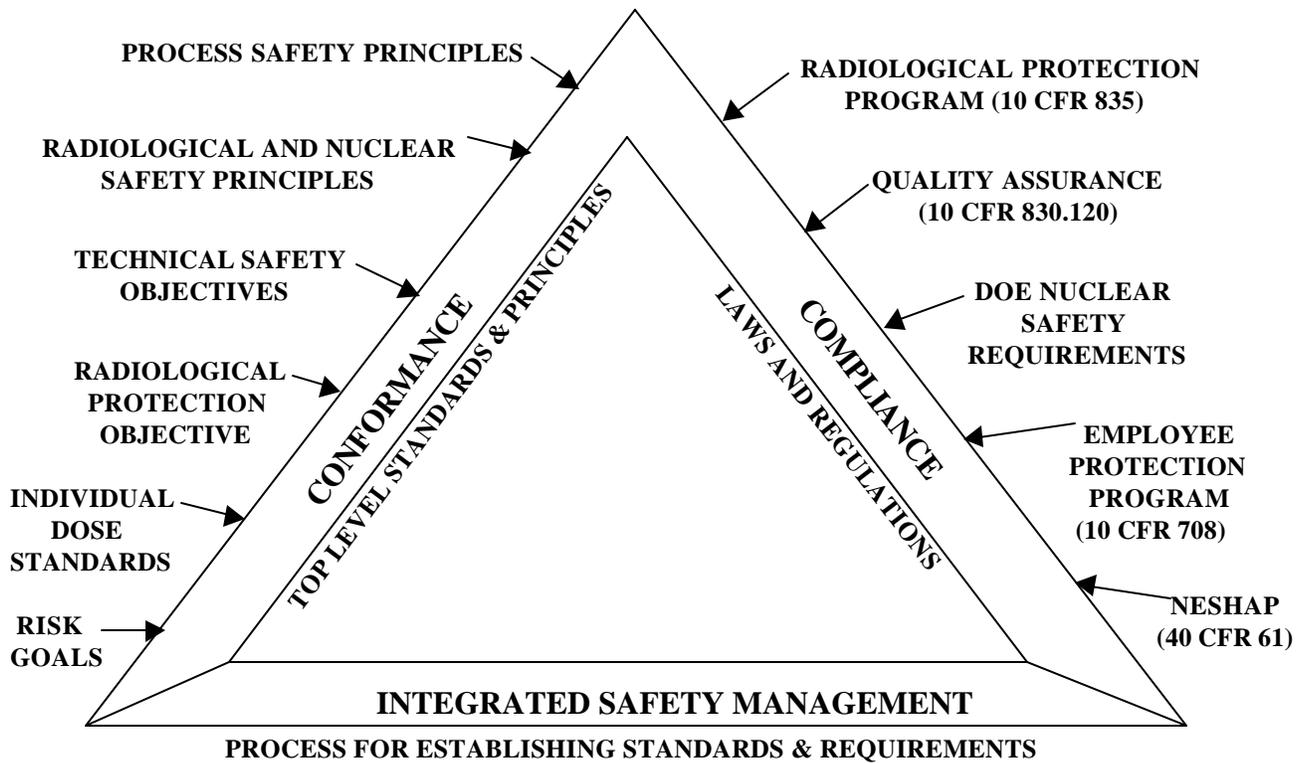
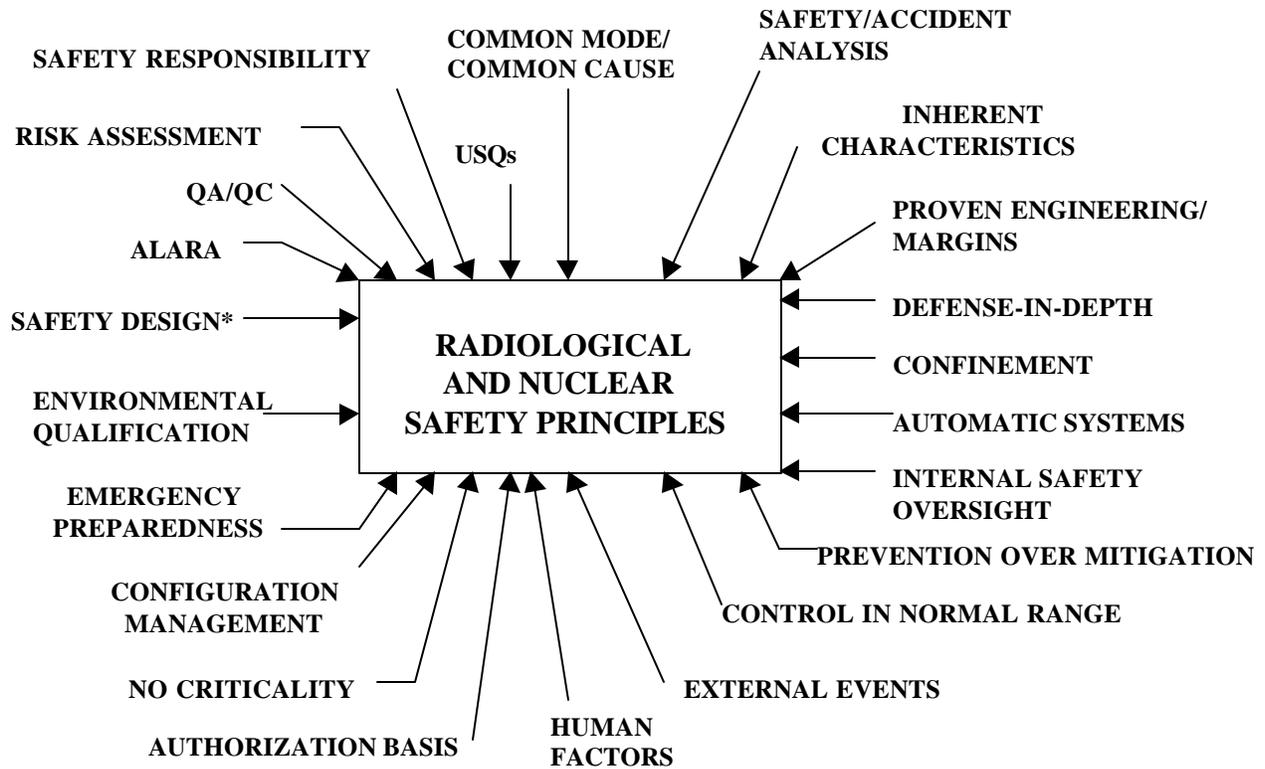
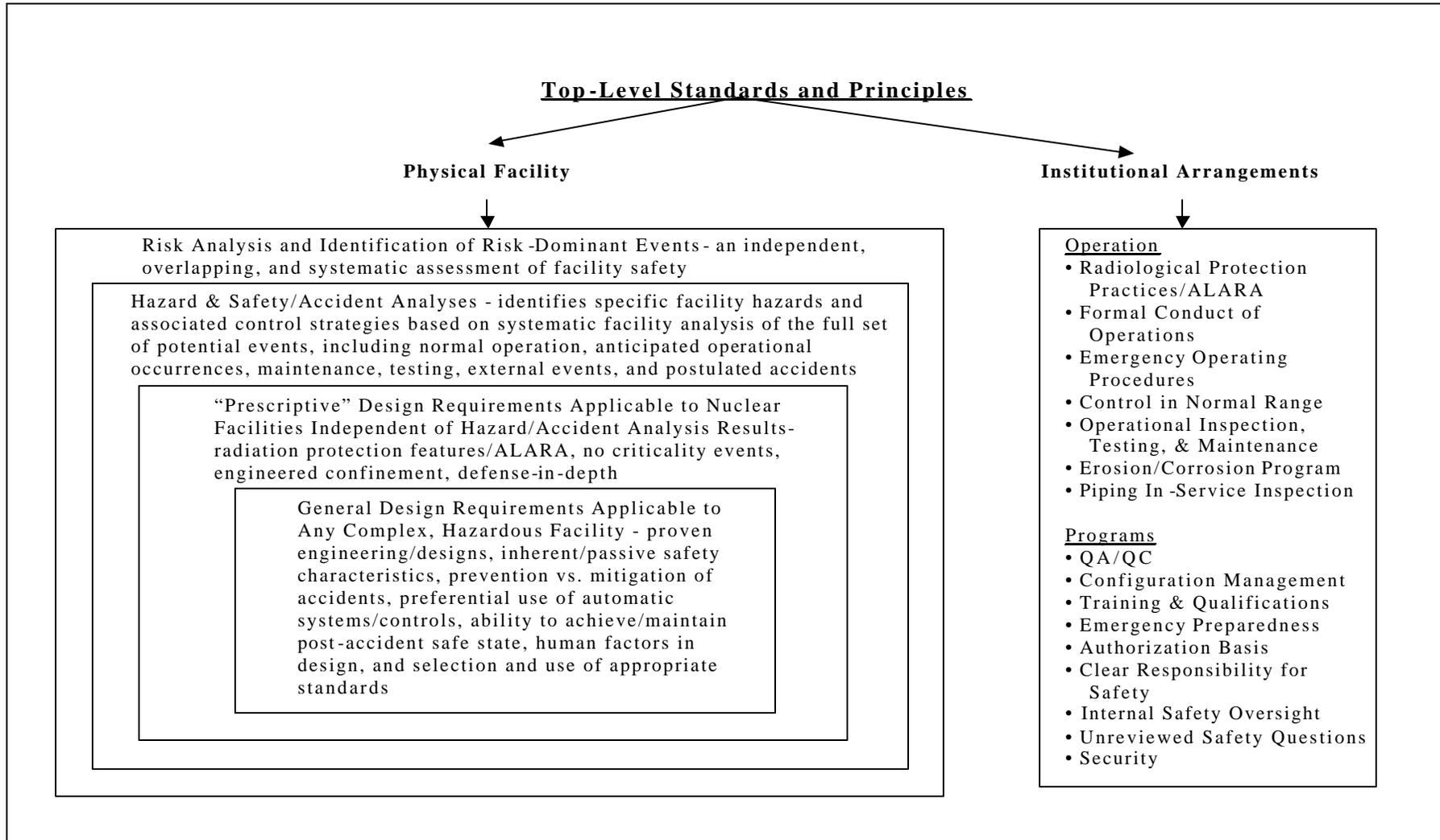


Figure 2. Radiological and Nuclear Safety Principles



* Facility designed for full set of events including: normal operation, anticipated operational occurrences, maintenance, testing, external events, and postulated accidents.

Figure 3. Top-Level Standards and Principles for Design, Construction, Pre-Operational Testing, Operation, and Safety Programs/Institutions



The RU continues to provide guidance to the RPP-WTP Contractor on implementation of the standards selection process through the review and comment on Contractor submittals and the conduct of topical meetings. A significant pertinent Contractor submittal, Design Safety Features, provided the RU with an integrated perspective on some of the individual important-to-safety structures, systems, and components (SSC) and examples of implementation of the standards identification process stipulated in DOE/RL-96-0004.

The emphasis of this position paper is on the requirements contained in the conformance leg of the safety triad, namely the top-level standards and principles stipulated in DOE/RL-96-0006. These top-level standards and principles include the individual dose standards, Radiological Protection/as low as reasonably achievable (ALARA) Objective, Risk Goals, Technical Safety Objectives, Radiological and Nuclear Safety Principles, and Process Safety Principles. These top-level standards and principles were derived from general safety principles developed for the New Production Reactor (NPR), DOE Orders, the U.S. Nuclear Regulatory Commission's (NRC) Advanced Reactor Safety Policy, Severe Accident Policy, and Safety Goal Policy; and the International Atomic Energy Agency's "Basic Safety Principles for Nuclear Power Plants" (INSAG-3). These are considered to embody much of the collective wisdom on nuclear safety that has accumulated worldwide from the operation of nuclear facilities over the past 50 years.

The top-level standards and principles are consistent with DOE nuclear safety policy as specified in Secretary of Energy Notice (SEN) 35-91, *Nuclear Safety Policy*. The historical development of these Top-Level Standards and Principles is addressed in another RU topic-specific study, RL/REG-98-23, *Bases for the Top-Level Standards and Principles and Glossary Definitions*.

It is worth noting that the three legs of the safety triad are not mutually independent. The conformance leg (top-level standards and principles) contains quality assurance and radiological protection requirements, somewhat redundant to the compliance leg (laws and regulations). As will be described later, the ISM leg incorporates many of the top-level standards and principles into the requirements and standards selection process. In subsequent sections of this position paper, when DOE/RL-96-0006 content is cited, it will be in italics.

3.0 DISCUSSION

This section describes:

- The laws and regulations related to radiological, nuclear, and process safety with which the RPP-WTP Contractor's ISM program must comply to achieve adequate safety.
- Top-level standards and principles that are implemented by RPP-WTP Contractor management programs and administrative processes and to which the Contractor's ISM program must conform to achieve adequate safety. These principles include Process Safety Principles which have proven to be effective in the chemical industry and have become the basis for accepted process safety practice. The Contractor will conform to these principles through implementation of their ISM program to address all process hazards associated with the Contractor's facilities.

Top-level standards and principles that are implemented by facility design, analysis, construction, and pre-operational testing, including principles integrated into the requirements and standards selection process.

3.1 Compliance with Laws and Regulations

The RPP-WTP Contractor's ISM program must ensure compliance with the laws and regulations applicable to the design and operation of RPP-WTP. Regulations applicable to the RPP-WTP include the DOE nuclear safety requirements, which derive their authority from the Atomic Energy Act and the Price-Anderson Amendments Act. DOE nuclear safety requirements are those regulations that are enforceable under 10 CFR 820 and include 10 CFR 830.120 "Quality Assurance Requirements" and 10 CFR 835 "Occupational Radiation Protection".

To comply with these laws and regulations, the Contractor has developed and implemented the following:

- An Employee Concerns Program (ECP) which implements portions of the provisions of 10 CFR 708 and is part of the facility authorization basis.
- A Quality Assurance Program and Implementation Plan (QAPIP)⁶, which complies with 10 CFR 830.120 and is part of the facility authorization basis.
- A Radiation Protection Program for design, which complies with 10 CFR 835 and is part of the facility authorization basis.

The RPP-WTP Contractor is also required by the Contract to limit radioactive and organic emissions from the vitrification facility. The National Emission Standards for Hazardous Air Pollutants (40 CFR 61, "National Emission Standards for Hazardous Air Pollutants", [NESHAP])⁷ limits the release of radioactivity from a DOE nuclear facility (e.g., the Hanford Site) to 10-mrem/year effective dose equivalent to any member of the public. Interface Description 22, Air Emissions, of the RPP-WTP Contract requires the RPP-WTP Contractor to maintain the exposure to the maximally exposed individual (non-acute exposure) as low as reasonably achievable, but not more than 1.5 mrem/year. Interface Description 22 also requires the RPP-WTP Contractor to maintain organic emissions from RPP-WTP as low as reasonably achievable, but not more than 0.375 tons per year.

⁶ The Contractor recently submitted his Quality Assurance Program (QAP) document, which was intended to replace the QAPIP.

⁷ NESHAP is not regulated by DOE.

3.2 Management System and Administrative Process Principles

3.2.1 Quality Assurance

All RPP-WTP activities important to radiological and nuclear safety, including those performed within the framework of the Contractor's ISM program, are required to comply with 10 CFR 830.120 and to conform with the requirements of the QAPIP (as per Section 3.1 above). *Quality assurance and quality control should be applied throughout all phases and to all activities associated with the facility as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet required standards.*⁸

Other Quality Assurance Principles to which the Contractor must conform are listed below. The Contractor is required to continue the quality assurance and quality control practices into procurement, construction, and operational activities for RPP-WTP by:⁹

- *Using well proven and established techniques and procedures supported by quality assurance practices to provide high quality equipment and achieve high quality construction.*
- *Establishing operational quality assurance and control programs to assist in ensuring satisfactory performance in facility activities important to safety.*

DOE/RL-96-0006 assigned special importance to the procedures and configuration management elements of quality assurance as is described in the following subsections. All of these quality assurance requirements are redundant to, and reinforce 10 CFR 830.120 requirements.

3.2.1.1 Procedures

Facility procedures are a quality assurance tool for ensuring compliance with requirements during the design, construction, operation, and deactivation of RPP-WTP. Overall Principles related to procedures to which the Contractor must conform, implemented within the framework of the ISM program, are as follows:¹⁰

- *Establish, document, and approve emergency operating procedures to provide a basis for suitable operator response to accident conditions.*
- *Develop and implement written operating procedures that provide clear instruction for safely conducting activities consistent with process safety information. The procedures should address at least the following elements: steps for each operating phase of the process, operating limits, safety and health considerations, and safety systems and their functions.*

⁸ DOE/RL-96-0006, Section 4.1.6.1.

⁹ Ibid., Sections 4.1.6.2 and 4.1.6.3.

¹⁰ DOE/RL-96-0006, Sections 4.3.1.3, 5.2.3, and 5.2.9.

- *Evaluate all planned changes involving the technology of the process and the facility design and operation in order to ensure that the impact on safety is analyzed and acceptable and to determine the need for modifications to operating procedures. The Contractor should establish and implement written procedures to manage changes to process chemicals, technology, equipment, and procedures; and changes to facilities. These procedures should address the technical basis for the proposed changes, impact of the changes on process safety, modification of the operating procedures, the schedule for proposed changes, and authorization for proposed changes.*

3.2.1.2 Configuration Management

A Configuration Management program for nuclear, radiological, and process safety of the RPP-WTP facility is required.¹¹ This program will ensure that during the design, construction, operation, and deactivation of RPP-WTP, the documentation of the design, administrative controls, procedures, operation, training, and maintenance of the facility remains accurate and retrievable.

Configuration Management Principles to which the Contractor must conform, implemented within the framework of the ISM program, are as follows:¹²

- *Formal configuration management should be applied to all facility activities during the program's lifetime to ensure that programmatic objectives related to radiological, nuclear, and process safety are fully achieved. Work should be performed and controlled according to pre-approved plans and procedures that clearly delineate responsibilities. Documented records should be retained.*
- *A system should be used to control and maintain accurate as-built drawings during the life of the facility related to radiological, nuclear, and process safety.*

3.2.2 Radiation Protection

RPP-WTP activities are required to comply with 10 CFR 835 and to conform to the requirements of the Radiation Protection Program (as per Sec. 3.1 above), including conformance with the Radiation Protection Objective. The Radiation Protection Objective requires the Contractor to *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 and within prescribed limits, and to ensure mitigation of the extent of radiation exposure and environmental impact due to accidents.*¹³

¹¹ BNFL-5193-QAP-01, Section 6.2.5.

¹² DOE/RL-96-0006, Sections 4.1.5.2 and 4.1.5.3.

¹³ Ibid., Section 3.2.

Radiation Protection Principles to which the Contractor must conform, implemented within the framework of the ISM program, during the operation and deactivation and decommissioning of RPP-WTP, are as follows:¹⁴

- *An acceptable system of radiation protection practices should be followed in the operational phase for the protection of workers and the public.*
- *The radiation protection staffs of the RPP-WTP Contractor's operating organization should establish written procedures for the control, guidance, and protection of personnel; and routinely monitor facility site radiological conditions, the exposure of facility personnel to radiation, and releases of radioactive effluents.*
- *Deactivation of the facility should be planned. These plans and provisions should incorporate radiation protection practices to protect Hanford site personnel and the public, both during and following deactivation activities; and waste minimization procedures to reduce the amount of radioactive waste generated during deactivation.*

3.2.3 Training

Personnel training and qualification serve an important role in achieving adequate safety by ensuring that RPP-WTP personnel have sufficient knowledge to safely fulfill the roles and responsibilities of their assigned tasks. Training and qualification have a direct impact on safety during design, construction, operation, and deactivation of the facility by:

- Improving technical ability
- Enhancing personal skills
- Increasing awareness of symptoms of potential hazardous situations in the workplace
- Increasing personal awareness of the potential impact of actions taken with regard to the safety of the individual, others, and the facility
- Establishing a safety culture that clearly assigns the responsibility for safety to the individual
- Reducing the probability of personnel error.

Personnel Training and Qualification Principles to which the Contractor must conform, implemented within the framework of the ISM program, are as follows:¹⁵

- *The Contractor operating organizations should become and remain familiar with the features and limitations of components included in the design of the facility. They should*

¹⁴ Ibid., Sections 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.3.2.1, 4.3.2.2, and 4.3.2.3.

¹⁵ Ibid., Sections 4.1.5.2, 4.3.4.1, 4.3.4.2, 4.3.4.3 and 5.2.4.

obtain appropriate input from the design organization on pre-operational testing, operating procedures, and the planning and conduct of training.

- *Personnel engaged in activities bearing on facility safety should be trained and qualified to perform their duties.*
- *Programs should be established for continual training of operations and maintenance personnel to enable them to perform their duties safely and efficiently.*
- *Operating staff should be trained and retrained in the procedures to follow if conditions exceed the design basis of the facility.*
- *Each operator should be trained in an overview of the process and in the operating procedures. The training should include emphasis on the specific safety and health hazards, operating limits, emergency operations, and safety work practices. The employees should receive refresher training at an appropriate frequency considering the applicable standards and the nature of the hazards.*

3.2.4 Facility Operation

A formal CONOPS program will be implemented by the RPP-WTP Contractor, including:

- Operation of the facility in accordance with Technical Safety Requirements (TSR)
- Establishment of high standards
- Communication of those standards to the workforce
- Provisions for sufficient qualified personnel to perform the activities necessary to meet the standards
- Implementation of a philosophy that workers and managers are accountable for their performance.

Sound CONOPS program practices are major contributors to the safety of the public and workers. Top-level principles to which the Contractor's CONOPS program must conform, implemented within the framework of the ISM program, are as follows:¹⁶

- *The RPP-WTP Contractor should exert full responsibility for the safe operation of the facility through a strong, unambiguous organizational structure.*
- *Operations should be conducted in accordance with approved technical safety requirements and in strict accordance with administrative and procedural controls.*

¹⁶ Ibid., Sections 4.3.1.1, 4.3.1.2, 4.3.1.4, 4.3.1.6, 4.3.1.7, and 4.3.1.8.

- *The facility manager should ensure that all elements for safe facility operation are in place, including an adequate number of qualified and experienced workers. Minimum requirements also should be set for the availability of staff and equipment.*
- *Limiting conditions of operation, limiting control settings, and safety limits should be established as necessary to ensure operation within the authorization basis.*
- *Throughout the life of the facility, the RPP-WTP Contractor should have access to engineering and technical support personnel, who are competent in all disciplines important to safety.*
- *Facility management should institute measures to ensure that events relevant to safety are detected and evaluated, and that necessary corrective measures are taken promptly and information on them is disseminated. Operational event reports should be prepared and submitted to the Director of the Regulatory Unit (Regulatory Official or RO). Facility management should have access to operational safety experience from other related facilities.*
- *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.*

The above principle¹⁷ is intended to minimize the wear and tear on the plant that is associated with normal operation while improving plant operability by restricting parameters to a set that becomes easily recognizable by the operator.

3.2.5 Emergency Planning

The development and implementation of an emergency management plan for the prompt, efficient, and effective response to emergencies in accordance with applicable local, state, and federal regulations is required. The emergency management plan is a significant element of the RPP-WTP Contractor's approach to safety due to its importance in ensuring the health and safety of the public and workers during emergency situations at the RPP-WTP facility. Development of the plan will be coordinated with other Hanford emergency management organizations and implementation will occur before radioactive or hazardous materials are introduced into the facility.

Principles related to emergency planning to which the Contractor must conform, implemented within the framework of the ISM program, are as follows:¹⁸

- *Emergency plans should be prepared before the startup of the facility, and should be exercised periodically to ensure that protection measures can be implemented in the*

¹⁷ Ibid., Section 4.1.1.3.

¹⁸ Ibid., Section 4.3.3.3 and 5.2.11.

event of an accident that results in, or has the potential for, unacceptable releases of radioactive materials within and beyond the facility control perimeter. Emergency planning zones defined around the facility should allow for the use of a graded response.

- *The Contractor should establish and implement an emergency action plan in accordance with the applicable standards.*

3.2.6 Unreviewed Safety Question Determinations

The implementation of internal safety oversight for the RPP-WTP facility to ensure the safety of the public and workers and to preclude environmental degradation is required. One of several oversight functions to be implemented is the unreviewed safety question (USQ) determination process. The USQ determination process is applied to proposed temporary or permanent changes to administrative and engineering controls to ensure the following:

- Probabilities of occurrence or consequences of accidents or malfunctions of important-to-safety equipment are not increased by the proposed change.
- New or different accidents or important-to-safety equipment malfunctions are not created by the proposed change.
- The margin of safety is not reduced by the proposed change.

A principle related to USQ determinations to which the Contractor must conform, implemented within the framework of the ISM program, is that *all facility modifications after operations begin that can affect safety should be assessed by the Contractor for an "unreviewed safety question" and positive determinations submitted to the RU for review.*¹⁹

3.2.7 Authorization Basis

The RPP-WTP regulatory process involves multiple steps of Contractor submittals and specific regulatory actions. Contractor submittals provide the information and commitments that serve as the basis for regulatory decisions taken by the RU in connection with regulatory actions and establish the RPP-WTP Authorization Basis. A principle related to the RPP-WTP Authorization Basis that the Contractor must conform to, implemented within the framework of the ISM program, is that *material that is part of the Authorization Basis should be established, documented, and submitted to the RU for evaluation and in support of decisions and regulatory oversight. The Contractor should maintain the material current with respect to changes made to the facility design and administrative controls and in the light of significantly new safety information.*²⁰

¹⁹ Ibid., Section 4.4.4.

²⁰ Ibid., Section 4.1.3.1.

It was found necessary to expand upon the Authorization Basis description in the Top-Level Standards and Principles and to provide for a process for change to ensure adequate control of this important area. To this end, the RU prepared RL/REG-97-13, *Regulatory Unit Position on Contractor-Initiated Changes to the Authorization Basis* that was subsequently invoked into the Contract by reference. The position paper describes the contents of the authorization basis and the procedures for amending it. It also delineates what changes the contractor can make on his own initiative and what changes require pre-approval by the RU.

3.2.8 Safety Responsibility/Culture/Oversight

As stated in the Contract,²¹ the RPP-WTP Contractor is responsible for providing safe and healthful working conditions for employees and all other persons under the Contractor's control who work in the general vicinity of the Contractor site, including subcontractors. The Contractor shall develop and implement an integrated program for conventional non-radiological worker safety and health; radiological, nuclear, and process safety; and environmental protection.

Principles for safety responsibility, culture, and oversight to which the RPP-WTP Contractor must conform, implemented within the framework of the ISM program, are as follows:²²

- *Responsibility for the safety of the facility rests with the RPP-WTP Contractor. In no way should this responsibility be diluted by the separate activities and responsibilities of designers, suppliers, constructors, the RU, or independent oversight bodies.*
- *The assignment and subdivision of responsibility for safety should be kept well-defined throughout the life of the facility.*
- *The RPP-WTP Contractor should assure commitments from relevant parties to provide data and services needed to fulfill its safety commitment.*
- *Operating experience and the results of research relevant to safety should be obtained, reviewed, and analyzed, and lessons that are learned should be implemented in the design, construction or modification, and operation of the facility.*
- *A safety/quality program should be established that governs the RPP-WTP Contractor's actions and interactions of all personnel and organizations engaged in activities related to the facility and emphasizes excellence in all activities. The Contractor should have safety and quality responsibilities specifically identified in its operations.*
- *Internal safety review procedures should be used by the RPP-WTP Contractor to provide a continuing surveillance and audit of facility operational safety and to support the facility manager in overall safety responsibilities.*

²¹ Contract No. DE-AC27-96RL13308, Standard 4.

²² DOE/RL-96-0006, Sections 4.1.2.1, 4.1.2.2, 4.1.2.3, 4.1.2.4, 4.1.4.1, 4.3.1.5, 4.4.1, and 4.4.2.

- *The RPP-WTP Contractor should establish a framework for its 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 should 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.*

3.2.9 Process Safety Principles

Process safety (i.e., safety from hazardous chemicals that may be in the waste provided to the RPP-WTP contractor or introduced into the treatment system as chemical agents) is incorporated into the RU's regulatory program because (1) chemical hazards are intimately bound to and co-exist with the radiological and nuclear hazards in the waste, (2) the regulatory approach to process safety incorporates consideration of OSHA/chemical industry safety principles in the standards selection process, and (3) the nuclear industry normally incorporates significant non-nuclear hazards with the evaluation of radiological and nuclear hazards, particularly if the non-nuclear hazards may affect the nature and the control of radiological and nuclear hazards. Incorporation of process safety into the RU regulatory programs means that chemical hazards and their control will be (1) evaluated by the RPP-WTP contractor and the RU concurrently with the evaluation of radiological and nuclear hazards, (2) included as aspects of the RU/contractor regulatory interactions, and (3) considered by the RU in arriving at its regulatory decisions. Incorporating process safety in the RU regulatory program ensures that adequate safety from radiological, nuclear, and chemical hazards is achieved in an integrated, consistent, and balanced manner.

The role of the hazards presented by various chemicals including releases, fires, and explosions, and the influence of those chemicals on radiological and nuclear hazards has become increasingly apparent as experience has accumulated from operations of nuclear facilities worldwide. To achieve adequate safety, it was decided that chemical process safety must be integrated into the overall safety approach used on the RPP-WTP. The safety classification of structures, systems, and components for chemical hazards assigned by the RPP-WTP contractor are based on the potential to exceed the Emergency Response Planning Guidelines (ERPG)-2 limits established by the American Industrial Hygiene Association (AIHA 1988) for members of the public, exceed the ERPG-3 chemical hazard exposure limits for co-located workers, or result in a single facility worker fatality or in-patient hospitalization of at least three facility workers (29 CFR 1904.8, "Reporting of Fatality or Multiple Hospitalization Incidents"). The Contractor is required to comply with the worker protection requirements in 29 CFR 1910 and 1926 (the Occupational Safety and Health Administration rules).

There are a total of 15 Process Safety Principles contained in DOE/RL-96-0006, most of which are similar to their radiological and nuclear safety counterparts and have been described above. These include principles associated with operating procedures, training, control over subcontractors, change control, incident investigation, emergency planning, compliance audits,

and pre-startup safety review. There are 3 of the 15 that are somewhat unique to process safety, and are repeated below.

3.2.9.1 Process Safety Information

The RPP-WTP Contractor should develop and maintain certain important information about the process. This information is intended to provide a foundation for identifying and understanding the process hazards. The process safety information includes, but is not limited to, a summary of material data, a description of each process and its operation, and equipment design data.

The information should confirm that the equipment is appropriate for the operation, that its integrity is maintained, and that it meets appropriate codes and standards.

3.2.9.2 Mechanical Integrity

The RPP-WTP Contractor should implement a mechanical integrity program that includes written procedures, training for maintenance activities, inspection and performance testing of process equipment, and quality assurance measures. The program should include measures to correct deficiencies in equipment that are outside acceptable limits.

Note: A mechanical integrity program is a major and necessary element in a process safety management program because of its importance in ensuring equipment integrity, eliminating potential ignition sources, and for determining that equipment is designed, installed, and operating properly.

3.2.9.3 Hot Work Control

The RPP-WTP Contractor should control hot work operations performed in or near the process or facility in order to ensure appropriate safety precautions, including fire prevention and protection, are taken prior to the work.

3.3 Facility Design, Analysis, Construction, and Pre-Operational Testing Principles

This section discusses the top-level standards and principles which must be conformed to by the RPP-WTP Contractor during the performance of design, analysis, construction, and pre-operational testing activities. These principles are presented as either general principles associated with facility design, analysis, construction, and pre-operational testing or principles that are integrated into the safety requirements and standards selection process (i.e., RL/REG-96-0004).

3.3.1. General Principles

General top-level standards and principles that the RPP-WTP Contractor must conform to when performing facility design, analysis, construction, and pre-operational testing activities include those associated with the Technical Safety Objectives, Risk Goals, confinement design, radiation protection program, human factors design/engineering, facility security and physical protection, construction authorization, and pre-operational testing.

3.3.1.1 Technical Safety Objectives

The technical safety objectives were derived from INSAG-3 (International Atomic Energy Agency report on the basic safety principles for nuclear power plants) technical safety objectives and a NPR document (general safety principles and requirements for the NPR “heavy water reactor” concept); tailored to reflect the regulatory approach developed for the RPP-WTP facility and the recognized need to ensure the adequacy of facility worker protection. The technical safety objectives²³ are cited below:

- *Measures in the design and operation of the facility to protect the public against accident conditions should be evaluated against acceptable guidelines to demonstrate that they perform their intended purpose with high confidence.*
- *Measures in the design and operation of the facility to protect the workers against accident conditions should be evaluated using an acceptable approach to demonstrate that they perform their intended purpose with high confidence.*
- *Particular care should be taken to identify, evaluate, and prevent and/or mitigate any vulnerabilities to accidents that might, by themselves, result in the release of radioactive material that exceeds acceptable levels.*

The first two of these technical safety objectives essentially require that design basis events be analyzed conservatively, as discussed in Section 3.3.2.1. The third objective has the effect of asserting that there is no acceptable level for accidental release of radioactive material from the facility for which there are no preventative or mitigative features. The objective mandates "particular care" for even those events that "might" result in release of material that exceeds acceptable levels. When combined with the requirement for conservative analyses and the requirement for confinement, the result is that preventative and/or mitigative measures are taken for all prospective events that could lead to the release of radioactive materials. There are no standards that legitimize some frequency of releases of radioactive material from the facility.

3.3.1.2 Risk Goals

The purpose of risk analysis and associated goals is to implement an alternate (to deterministic safety analysis), systematic method for assessing the safety of the facility design. One of the

²³ DOE/RL-96-0006, Section 3.3.

benefits of establishing risk goals is to restrict the numbers of kinds of off-normal events that can occur in any period. Without risk goals, it would be theoretically²⁴ possible to have hundreds of different kinds of events, each with a probability of occurrence of 10^{-2} /year, and each leading to an exposure of the public of 5 rem. In contrast to design basis event analyses, risk analyses are performed on a best estimate basis and include hypothetical events with probabilities less than 10^{-6} per year. A method acceptable to the RU for demonstrating conformance with these risk goals is described in RU Position Paper DOE/REG-2000-08, *Regulatory Unit Position on Conformance with Risk Goals in DOE/RL-96-0006*. The specific risk goals selected for the RPP-WTP are:²⁵

- *The Operations Risk Goal requires the risk to the population (public and workers) in the area of the Contractor's facility, of cancer fatalities that might result from facility operations, 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. For evaluation purposes, individuals are assumed to be located within 10 miles of the controlled area.*
- *The Accident Risk Goal requires 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. For evaluation purposes, individuals are assumed to be located within 1 mile of the controlled area.*
- *The Worker Accident Risk Goal requires 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. For evaluation purposes, workers are assumed to be located within the controlled area.*

3.3.1.3 Confinement

Potentially contaminated gaseous releases from the facility must be filtered so as to remove radioactive material before release to the environment. While it is acknowledged that some tiny fraction of radioactive material that enters the filters may escape filtration, the basic concept inherent in the following confinement principle is that there is no acceptable release of radioactive material to the environment from which a go/no go decision is made to include a confinement system in the facility design.

The facility should be designed to retain 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.

²⁴ "Theoretical" requires emphasis in this instance. For the reasons stated in Section 3.3, the potential for there being hundreds of events with 10^{-2} occurrence probabilities, each leading to 5 rem of exposure to the public, is non-existent.

²⁵ DOE/RL-96-0006, Sections 3.1.1, 3.1.2, & 3.1.3.

Note that this Principle requires the retention of essentially all radioactive material, not just that greater than some specified limit. The confinement is provided to minimize releases of radioactive material from the facility without regard for the magnitude of the release.

3.3.1.4 Radiation Protection

As noted in Sec. 3.2.2, RPP-WTP activities are required to comply with 10 CFR 835 and to conform to the requirements of the Radiation Protection Program. Per Table 1, the ALARA design objective for normal facility events is set at ≤ 1.0 rem/year for both the worker and co-located worker, which is consistent with 10 CFR 835.1002(b). Importantly, 1.0 rem/event has also been established as the design action threshold for anticipated events for both the worker and co-located worker. This extension of 1.0 rem/event for anticipated events is identified in the dose standards²⁶ in the top-level standards and principles as an ALARA design objective. The effect of imposing this 1.0 rem/event into the anticipated events regime is to establish an action threshold for radiation exposures above which specific justification for increased exposures is required. This requirement from DOE/RL-96-0006 goes beyond that which would be required by 10 CFR 835.

Radiation Protection Principles to which the Contractor must conform during RPP-WTP design, analysis, construction, and pre-operational testing, implemented within the framework of the ISM program, are as follows:²⁷

- *The Contractor is expected to follow an acceptable system of radiation protection practices in the design, construction, and pre-operational testing phases of the facility for the protection of workers and the public.*
- *At the design stage, the Contractor should incorporate radiation protection features to protect workers from radiation exposure and to keep emissions of radioactive effluents as low as reasonably achievable and within prescribed limits. As noted earlier, the Contract-prescribed limit for RPP-WTP, which is derived from NESHAP requirements, is as low as reasonably achievable, but not more than 1.5 mrem per year to the maximally exposed member of the public (non-acute exposure).*
- *The design of the facility should incorporate provisions to facilitate deactivation and the final decommissioning. The objective of these provisions should be to reduce radiation exposures 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.*

²⁶ Although Table 1 is identified as dose standards above normal background, the dose consequence values in the table are effectively acceptance criteria for the conservative analysis of hypothetical, worst-case scenarios of classes of events with the specified occurrence probabilities.

²⁷ Ibid., Sections 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.3.2.1, 4.3.2.2, and 4.3.2.3.

Table 1. Dose Standards Above Normal Background

Description	Estimated Probability of Occurrence $f(\text{yr}^{-1})$	General Guidelines	Worker	Co-located Worker	Public
<u>Normal Events</u> : Events that occur regularly in the course of facility operation (e.g., normal facility operations).	$f > 0.1$	Normal modes of operating facility systems should provide adequate protection of health and safety.	<p>~ 5 rem/yr</p> <p>~ 50 rem/yr any organ, skin, or extremity</p> <p>~ 15 rem/yr lens of eye</p> <p>~ 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b)⁽¹⁾</p>	<p>~ 5 rem/yr</p> <p>~ 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b)⁽¹⁾</p>	<p>~ 10 mrem/yr (airborne pathway)</p> <p>~ 100 mrem/yr (all sources)</p> <p>~ 100 mrem/yr (public in the controlled area)</p> <p>~ 25 mrem/yr (radioactive waste)</p>
<u>Anticipated Events</u> : Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	$10^{-2} < f \sim 10^{-1}$	The facility should be capable of returning to operation without extensive corrective action or repair.	<p>~ 5 rem/event^(2, 3)</p> <p>1.0 rem/event design action threshold⁽⁴⁾</p>	<p>~ 5 rem/event^(2, 3)</p> <p>1.0 rem/event design action threshold⁽⁴⁾</p>	~ 100 mrem/event ⁽³⁾
<u>Unlikely Events</u> : Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	$10^{-4} < f \sim 10^{-2}$	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 1. Dose Standards Above Normal Background (cont.)

Description	Estimated Probability of Occurrence $f(\text{yr}^{-1})$	General Guidelines	Worker	Co-located Worker	Public
<u>Extremely Unlikely Events:</u> 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.	$10^{-6} < f \sim 10^{-4}$	Facility damage may preclude returning to operation.	~ 25 rem/event ^(2,3)	~ 25 rem/event ^(2,3)	~ 25 rem/event ~ 5 rem/event target ~ 300 rem/event to thyroid
<u>Location of Receptor</u> ²⁸			Within the the Contractor's RPP-WTP Controlled Area Boundary, including AP 106	The most limiting location at or beyond the Contractor's RPP-WTP 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 co-located 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 co-located 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 Contractor's 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.

²⁸ This subject is further discussed in RL/REG-2000-07, *Regulatory Position on Acceptability of the TWRS-Privatization Dose Standards for Unlikely and Extremely unlikely Events*, and RL/REG-2000-08, *Regulatory Position on Conformance with Risk Goals in DOE/RL-96-0006*.

3.3.1.5 Human Factors

The following Principles are intended to acknowledge the fallibility of human beings and the checks and balances that, therefore, need to be a part of the overall safety approach.²⁹ The common thread in the Human Factors Principles is the acknowledgement of the possibility of error. The incidence of error can be reduced by appropriate design, adequate training and qualifications, and operating limits or administrative controls. The effects of errors that occur regardless can be reduced by a quality assurance (QA) program or internal safety reviews.

- *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.*
- *The possibility of human error in facility operations should 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.*
- *Sufficient instrumentation and control capability should be provided so that under normal operating and postulated accident conditions the operators can diagnose facility conditions, place and maintain the facility in a safe state, and mitigate accidents. If necessary, measures should be provided to protect the operator in the performance of these functions.*
- *Parameters to be monitored in the control room should be selected and their displays should be arranged to ensure that operators have clear and unambiguous indications of the status of facility conditions important to safety, especially for the purpose of identifying and diagnosing the actuation and operation of a system or components important to safety.*

3.3.1.6 Facility Security and Physical Protection

The following Principle recognizes the need to control access to the RPP-WTP facility and to protect those facility assets relied upon in the safety basis to ensure that facility safety is not compromised.³⁰

- *Adequate provisions for facility security and physical protection of SSC important to safety should be provided.*

²⁹ Ibid., Sections 4.1.1.6, 4.2.6.1, 4.6.2.2, 4.6.2.3.

³⁰ Ibid., Section 4.3.6.1.

3.3.1.7 Safety Issue Assessment and Resolution

The following Principle recognizes the importance to safety of maintaining discipline in the design and construction of RPP-WTP through the timely and thorough assessment and resolution of safety issues.³¹

- *The RPP-WTP 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.*

3.3.1.8 Pre-Operational Testing

A thorough pre-operational testing program is required to validate that the design, construction, hardware, programs, and personnel are ready to support safe operation of the facility. This testing will ensure that the equipment and facility are properly built and will operate as designed before transition to the operational phase. The program will also be used to document the as-built configuration and the initial operating parameters of the facility. Pre-operational testing supports the performance of a final system analysis and confirmation of the adequacy of training and facility operating procedures.

Principles related to pre-operational testing to which the Contractor must conform, implemented within the framework of the ISM program, are as follows:³²

- *A pre-operational testing program should be established and followed to demonstrate that the entire facility, especially items important to safety, have been constructed and function according to the design intent, and to ensure that weaknesses are detected and corrected.*
- *Procedures for normal facility and systems operation and for functional tests to be performed during the operating phase should be validated as part of the pre-operational testing program.*
- *During pre-operational testing, detailed diagnostic data should be collected on systems and components important to safety and the initial operating parameters of the systems and components should be recorded.*
- *During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components important to safety should be determined and documented. Operating points should be adjusted to conform to values in the design basis. Training procedures and limiting conditions for operation should be modified to accurately reflect the operating characteristics of the systems and components as built.*

³¹ Ibid., Section 4.4.3.

³² Ibid., Sections 4.2.8.1, 4.2.8.2, 4.2.8.3, and 4.2.8.4

3.3.2 Principles Influencing Safety Requirements and Standards Selection

The RPP-WTP Contractor has implemented an ISM program to accomplish the comprehensive and consistent analysis of hazards associated with the RPP-WTP design and operation, selection and confirmation of control strategies to prevent or mitigate hazardous situations, and the identification of safety standards and requirements tailored to the hazards associated with the Contractor's waste treatment services. This program provides the framework for ensuring compliance with the applicable laws and regulations and conformance with DOE/RL-96-0006, such that adequate safety is achieved in the design and operation of RPP-WTP.

The following sections discuss how selected elements of the Contractor's ISM program provide the framework for ensuring conformance to the technical/process requirements of DOE/RL-96-0006. The selected ISM elements include:

- Hazard evaluation/hazard analysis
- Control strategy selection and development (associated with safety features identification and augmentation)
- Identification of important to safety SSC.

3.3.2.1 Hazard Evaluation/Hazard Analysis

The RPP-WTP Contractor's hazard evaluation/analysis process includes hazard identification, definition of hazardous situations and accident sequences, and assessment of unmitigated consequences. The hazard evaluation/analysis performed by the RPP-WTP Contractor estimates the potential consequences from unmitigated hazardous situations and accident sequences to facility workers, co-located workers,³³ and members of the public. For events involving a potential radiological release, a severity level (SL) is assigned based on the unmitigated consequence assessment. The severity levels are used by the RPP-WTP Contractor as part of the approach to tailoring of safety in the standards identification process. Four severity levels are used for RPP-WTP (Table 2).³⁴

³³ RL/REG-98-18, *Regulatory Unit Position on Radiological Safety for Hanford Co-Located Workers*.

³⁴ *Safety Requirements Document (SRD)*, BNFL-5193-SRD-01, Volume II, Appendix A, BNFL Inc., 1998.

Table 2. Accident Severity Level Identification

SL	Facility Worker Consequence	Co-Located 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

The accident severity levels in Table 2 are related to the radiation dose standards (Table 1). Table 1 identifies the human (worker, co-located worker, and members of the public) dose standards to which all activities of the RPP-WTP Contractor involving radiological and nuclear hazards must comply, based on conservative estimation of event consequences and frequencies, after application of control strategies. Table 1 is drawn from the Contractor's SRD and is derived from a similar table of dose standards as those contained in DOE/RL-96-0006. Table 1 and DOE/RL-96-0006 are fully consistent with the exception of a nuance of interpretation on the application of ALARA to Anticipated Events. Also, Table 1 has quantified entries that are identified as TBD in the DOE/RL-96-0006. These standards are consistent with radiological exposure limits embodied in DOE and NRC regulations and the perspectives of the International Council on Radiological Protection. The basic principle behind the definition of accident severity levels is that the greatest degree of protection (both prevention and mitigation) needs to be afforded to the events that have the most severe potential consequences. This principle is fully consistent with the concept of tailoring.

From a comparison of Tables 1 and 2, the following conclusions are evident:

- Unmitigated consequences associated with SL-1 events exceed the radiological dose standards for extremely unlikely events,
- Unmitigated consequences associated with SL-2 events are below the radiological dose standards for extremely unlikely events,
- Unmitigated consequences associated with SL-3 events are below the radiological dose standards for unlikely events, and
- Unmitigated consequences associated with SL-4 events are below the radiological dose standards for anticipated events.

An obvious question that can be raised about the approach reflected in Tables 1 and 2 is the extent to which the sharp transitions in dose standards, as one moves across the event frequency domain, introduce anomalies in the resulting analyses. However, for the following reasons, the frequency/consequence relationship for accident events approved as part of the Preliminary Safety Analysis Report (PSAR) by the RU will tend to be more linear:

- The SRD requires that, in addition to meeting the listed exposure standards for accidents, the RPP-WTP Contractor's approach to accident mitigation is to evaluate accident consequences to ensure that the calculated exposures are far enough below the dose standards to account for uncertainties in the analysis, and to provide for sufficient design margin and operational flexibility.
- The analysis performed is required to be conservative. This contrasts with the risk analysis, discussed later in this paper, which is performed on a nominal basis. A natural consequence of conservative analyses is that events, which are close to a boundary in the frequency domain, will be analyzed in the lower frequency bin.

The effect of the above is to move event consequences or frequencies away from the thresholds and toward the center of the frequency bins, reducing the step-wise relationship to more of a continuum.

Another issue possibly raised by this approach is the extent to which it is adversely affected by individuals with built-in biases who are choosing the event frequencies. The RPP-WTP Contractor selects event frequencies after consulting a database of comparable events. They are not, therefore, the product of judgment alone and must be supported by quantitative data. The resulting analyses are then incorporated into the Contractor's Hazard Analysis Report and Safety Analysis Report, both of which are parts of the authorization basis and subject to RU approval. The regulatory involvement in the process, therefore, establishes a second check and balance against bias in the selected frequencies.

Principles to which the Contractor must conform when performing hazard evaluations, implemented within the framework of the ISM program, are as follows:³⁵

- *The Contractor should perform a process hazards analysis using acceptable industry practices. The process hazards analysis should be appropriate for the complexity of the process and the hazard. The Contractor should consider the effects of engineering and administrative controls, human factors, facility siting, and previous incidents in the hazard analysis. The Contractor should document the results of the hazards analysis including process hazards and possible safety and health effects. The Contractor should submit the results of the hazards analysis to the RU for evaluation and in support of authorization decisions and regulatory oversight.*
- *One of the purposes of the hazard analysis is to evaluate the adequacy of the design and operating procedures. The Contractor should establish a system to address any findings from this evaluation in order to assure that the equipment and procedures provide an adequate degree of protection against accidents.*
- *The Contractor should review and update the hazard analysis periodically to assure that the process hazards analysis is consistent with the current process.*

³⁵ DOE/RL-96-0006, Section 5.2.2.

3.3.2.2 Control Strategy Selection and Development

The RPP-WTP Contractor's process for control strategy selection and development includes the following:

- Identification of candidate control strategies based upon the unmitigated consequence results of the hazard analysis
- Selection and confirmation of preferred control strategies
- Identification of important-to-safety SSC based on the results of safety/accident analyses
- Identification of performance requirements and assumptions for the important-to-safety SSC.

Both the selection and confirmation of preferred control strategies and the identification of important-to-safety SSC activities of the Contractor's ISM program require conformance to Principles involving technical/process requirements to achieve adequate safety. These ISM program activities are discussed in greater detail in the following sections.

3.3.2.2.1 Selection of Preferred Control Strategies

The RPP-WTP Contractor is required to conform to DOE-specified General Radiological and Nuclear Safety Principles³⁶ in the design and operation of the vitrification facility. Many of these radiological and nuclear safety principles, directed at protecting the public and workers and mitigating accident vulnerabilities, are used by the RPP-WTP Contractor during the selection of preferred control strategies to determine: (1) the effectiveness in achieving the expected level of safety, and (2) the need for additional measures. Those used explicitly in the control strategy selection process are described below.

Preferential Use of Passive Control Strategies

A Principle that the RPP-WTP Contractor must conform to within the framework of the ISM program is that *design features that enhance safety through simplified, inherent, passive, or other highly reliable means to accomplish safety functions should be employed to the maximum extent practicable.*³⁷

Preferential Use of Preventative Control Strategies

The preferential use of preventative vs. mitigative control strategies is embodied in the following Principles:³⁸

³⁶ Ibid., Section 4.0.

³⁷ Ibid., Section 4.2.5.

³⁸ Ibid., Sections 4.1.1.2 and 4.2.2.5.

- *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.*
- *The facility should be designed and operated in a manner that prevents nuclear criticality.*

Use of Automatic Systems for Safety

The following principle from DOE/RL-96-0006 is conventional practice in the design of nuclear facilities and has been practiced since the earliest production facilities. It is one of the first lines of defense against the development of potentially unsafe conditions.³⁹

- *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 set points.*

Existing Design

The existing design control strategy selection criterion is directed at selecting existing and/or proven control strategies, which are verified by the ISM program to be properly applied to the hazardous situation and whose control strategy elements are tailored commensurate with the potential magnitude of the hazard. The selection of existing and/or proven control strategies, implemented within the framework of the ISM program, must conform to the following Principles:⁴⁰

- *The Contractor should use well proven and established techniques and procedures supported by quality assurance practices to provide high quality equipment and achieve high quality construction.*
- *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.*

Reliability, Availability, Maintainability, and Inspectability (RAMI)

The RAMI control strategy selection criterion must be applied within the framework of the ISM process in conformance with the following Principles.⁴¹

- *Codes and standards for 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 an unacceptable release of radioactivity during the operational life of the facility.*

³⁹ Ibid., Section 4.1.1.5.

⁴⁰ Ibid., Sections 4.1.6.2 and 4.2.2.1.

⁴¹ Ibid., Sections 4.2.2.4, 4.2.7.1, 4.2.7.2, and 4.3.5.1.

- *Reliability targets should be assigned to structures, systems, and components or functions important to safety. The targets should be consistent with the roles of the structures, systems, and components or functions in different accident conditions. Provision should be made for appropriate testing and inspection of structures, systems, and components for which reliability targets have been set.*
- *Structures, systems and components important to safety should be designated, designed and constructed for appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.*
- *Structures, systems, and components important to safety should be the subject of appropriate, regular preventive maintenance, inspection, and testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the life of the facility. Such activities should be carried out in accordance with written procedures supported by quality assurance measures.*

Common Cause/Common Mode

The RPP-WTP Contractor's ISM program considers common cause/common mode failures in the hazards analysis and in the identification and selection of preferred control strategies. The analysis of common cause/common mode events focuses on identifying provisions to prevent the loss of safety functions. Common cause events to be considered in the hazards analysis and selection of preferred control strategies include the following:

- Natural phenomena events
- External man-made events
- Loss of electrical power
- Loss of control or instrument air
- Fire
- Internal missiles
- Internal flooding.

The analyses of natural phenomena events will consider induced effects, such as fire and loss of electrical power.

Common-mode failures are 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.⁴²

As part of the process for selecting preferred control strategies within the RPP-WTP Contractor's ISM program, common cause and common mode contributions to the event sequences and any control strategy requirements to mitigate these effects are assessed. This assessment involves the consideration of three broad categories of dependencies to classify and define common cause and

⁴² Ibid., Section 6.0.

common mode failures. Each category represents a functionally different way in which commonalities between redundant systems, trains or components can potentially reduce their overall expected reliability and are defined as follows:

- Functional dependencies which reflect the reliance of multiple systems, trains, or components on a single system, train, or component or process condition, resulting in the potential for common cause failures. Defense from common cause failures due to functional dependencies comes primarily from their overt recognition during the design phase (i.e., formal, structured hazard analysis and control strategy development) and assessment of their explicit contribution to process failures and their effects on safety prior to acceptance.
- Spatial dependencies between otherwise independent pieces of equipment that originate from their relative locations and the potential for physical interactions or common loss (i.e., the potential for common cause failures). Defense against common cause failures due to spatial dependencies comes from hardening or protecting each component to make it less vulnerable to the specific hazard of concern and from physical separation to minimize the likelihood of multiple failures from a single casualty.
- Institutional dependencies (also called common mode failures) that result from activities within the facility by maintainers, operators, designers, or equipment manufacturers which result in the near-simultaneous failure of otherwise independent components. Defenses against common mode failures include the use of functionally diverse equipment, staggered maintenance for independent channels/trains of equipment, post-maintenance and testing requirements, configuration management controls, and personnel training and awareness.

The RPP-WTP Contractor's search for functional and spatial dependencies between independent systems uses the hazards identification and assessment process. This is done primarily with the use of hazard and operability (HAZOP) analysis guidewords, which specifically address consequential (dependent) failures, which result from, or follow, an initiating event. Because of the large number of potential opportunities for the institution to implicitly contribute to common cause failure potential, the Contractor's assessment of institutional dependencies involves a statistical approach to describe the aggregate effects of institutional dependencies. This approach involves combining failure coupling factors which have been derived from actual nuclear plant experience with the independent hardware failure probabilities to estimate the probability of near-simultaneous failure of redundant and functionally independent components or trains.

The common cause/common mode control strategy selection criterion must be applied in conformance with the Principle,⁴³ implemented within the framework of the ISM program, that *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.*

⁴³ Ibid., Section 4.2.2.2.

Defense-in-Depth

The expression “defense-in-depth” has been widely used within the nuclear industry and has evolved to include a variety of meanings. In its broadest form, it could be interpreted in the same sense that the term “adequate safety” is being used in this position paper. The RPP-WTP Contractor has effectively chosen a relatively narrow definition as described in this section. The RU considers the matter to be essentially one of semantics and has no particular position on how the term is defined, so long as it is well-defined. It is pointed out that the authors of DOE/RL-96-0006 chose to group prevention, control, confinement, automatic systems, and human aspects under defense-in-depth. While the Contractor has proposed implementing subordinate standards for all of DOE/RL-96-0006 defense-in-depth requirements, the focus of the defense-in-depth strategy appears to be on the determination of the number of independent physical barriers, the application of the single failure criterion, and the target frequency for the unmitigated event.

The Contractor's approach begins with the concept of accident severity level which reflects the unmitigated consequences of a postulated accident. Table 2, introduced earlier in Section 3.3.2.1, identifies four levels of severity as a function of unmitigated event consequences to the worker, co-located worker, and the public. Since the exposures in Table 2 exceed the dose standards from Table 1, the systems, structures, and components (SSCs) that are necessary to prevent or mitigate these events, are all designated as important to safety.⁴⁴ Table 3, also drawn from the SRD,⁴⁵ then imposes control strategy requirements on the important-to-safety SSCs as a function of severity level.

In Appendix B of the SRD, the RPP-WTP Contractor has committed that, when active SSC are required to achieve defense-in-depth, the single failure criterion will be applied according to Table 3. When application of the single failure criterion is required (SL-1 events) or considered to be appropriate by the RPP-WTP Contractor (selected SL-2 events), the Contractor will follow the requirements of ANSI/ANS-58.9 for fluid systems and IEEE Standard 379 for electrical and instrumentation and control systems. The application of the single failure criterion begins with identification of an initiating event within the framework of the ISM process. In evaluating the defense-in-depth of the facility, single failures are to be postulated in addition to the initiating event. For fluid systems, during the short term, the single failure considered may be limited to an active failure. During the longer 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.⁴⁶

The hazard severity levels shown in Table 2 are a measure of the consequences from unmitigated events; that is, prior to incorporating SSC that prevent or mitigate the event. Following the selection of a preferred control strategy, 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 mitigated event frequency. Verifying that the event frequency is less than the target frequency

⁴⁴ SRD, Appendix A, Section 6.0. A more extensive treatment of important to safety follows in Section 3.3.2.3.

⁴⁵ SRD, Appendix B, Section 3.0.

⁴⁶ SRD, Appendix B, Section 2.1.2.

shown in Table 3⁴⁷ provides one confirmation that, in addition to the other specific defense-in-depth measures discussed below, the chosen control strategy includes sufficient SSC to adequately implement defense-in-depth in a graded approach.

The defense-in-depth control strategy confirmation criterion must be applied in conformance with the following Principle⁴⁸ and implemented within the framework of the ISM program (Note that the principle has been broadly worded):

- *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, no 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.*

Table 3. Implementation of Defense-in-Depth by SSC

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	At least one physical barrier.	<10 ⁻¹

3.3.2.2.2 Confirmation of Preferred Control Strategies

After the identification of preferred control strategies, taking into consideration the radiological, nuclear, and process safety requirements discussed in Section 3.3.2.2.1, the RPP-WTP Contractor will confirm the selection by:

- Selecting a set of representative design basis events (DBEs) to be used to establish the performance requirements for important-to-safety SSC. DBEs are defined as those postulated events which provide bounding conditions for establishing the performance requirements for SSC that are necessary to:
 - Ensure the integrity of the safety boundaries protecting the worker
 - Place and maintain the facility in a safe state indefinitely

⁴⁷ SRD, Volume II, Appendix B, Section 3.0.

⁴⁸ DOE-RL-96-0006, Sections 4.1.1.1.

- Prevent or mitigate the event consequences so that the radiological exposures to the general public or the workers would not exceed appropriate limits (Table 1).

The DBEs also establish the performance requirements for SSC whose failure under DBE conditions could adversely affect any of the above functions.

The set of DBEs includes selected events from the hazardous conditions identified during the hazard analysis, prescribed natural phenomena hazard events, and man-made external events. The DBEs selected for detailed accident analysis include all scenarios necessary to envelope the conditions for establishing performance requirements for important-to-safety SSC. They also represent a distillation of hazard control strategies to those that are necessary to establish the design basis while retaining sufficient fine structure to permit adequate tailoring.

- Performing accident analyses to calculate the mitigated consequences and frequencies for which the control strategies provide a preventive or mitigative function.
- Based upon the results of the accident analysis, determining if the preferred control strategy:
 - satisfies defense-in-depth requirements
 - meets the frequency target for the unmitigated severity level (Table 3).

Meeting the target frequency, after accounting for conservative estimations of mitigating effects, ensures that the radiological dose consequences to workers, co-located workers, and members of the public will be well-within the radiation dose standards (Table 1), as discussed earlier (Section 3.3.2.1).

If both the defense-in-depth requirements and the severity level frequency target are satisfied, the preferred control strategy is confirmed as acceptable for subsequent determination of important-to-safety structures, systems, and components and the identification of associated performance requirements.

3.3.2.3 Identification of Important-to-Safety SSC

Important-to-safety SSC are defined⁴⁹ as those 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 DOE/RL-96-0006 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 SSC that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent

⁴⁹ DOE/RL-96-0006, Section 6.0.

demands on or adversely affect the performance of safety functions⁵⁰ if they fail or malfunction, i.e., support systems, subsystems, or components. The support systems, subsystems, or components would be subject to applicable top-level 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 facility design 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 assessment identify vulnerabilities resulting from non-safety-related equipment, additional SSC should be considered for inclusion within this definition.

Principles that must be conformed to as part of the determination of important-to-safety SSC, including the safety/accident analyses upon which this determination is based, and implemented within the framework of the ISM program, are as follows:

Safety/Accident Analysis⁵¹

- *The facility should be designed for a set of events such as: normal operation, including anticipated operational occurrences, maintenance, and testing; external events; and postulated accidents.*
- *Acceptable risk analyses should be applied during the design to delineate provisions for the prevention and mitigation, including emergency preparedness and response, of otherwise risk-dominant events.*
- *A safety analysis should be carried out as required to evaluate the safety performance of the design and identify requirements for operations.*
- *Hanford Site and offsite mitigation measures should be provided to substantially reduce the effects of an unacceptable accidental release of radioactive material.*
- *The results of analyses of the response of the facility 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 facility control perimeter (security fence) should be used in preparing guidance on an accident management strategy.*

Environmental Qualification⁵²

- *Structures, systems, and components important to safety should be designed and qualified to function as intended in the environments associated with the events for which they are*

⁵⁰DOE/RL-96-0006, Section 6.0. Safety functions are defined as any functions 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.

⁵¹ Ibid., Sections 4.2.1.1, 4.2.1.2, 4.2.1.3, 4.3.3.1, and 4.3.3.2.

⁵² Ibid., Section 4.2.2.3.

intended to respond. The effects of aging on normal and abnormal functioning should be considered in design and qualification.

Safe State Capability⁵³

- *The facility design should provide additional capability to place and maintain the facility in a safe state following an accident if the normal control areas are expected to become uninhabitable.*

4.0 POSITION

Based on the discussion in Section 3 of compliance with legal and regulatory requirements, conformance with DOE/RL-96-0006, and adherence to the contract-prescribed process for establishing safety standards and requirements, the RU has established the following positions on the achievement of adequate safety for RPP-WTP design and operations.

- 4.1 Compliance with applicable laws and regulations, conformance with DOE-specified top-level standards and principles, and implementation of the contractually prescribed process for requirements and standards selection, as presented in Section 3, provide comprehensive and diverse assurance that adequate safety will be achieved in the design, construction, and operation of the RPP-WTP vitrification facility.
- 4.2 Comprehensive assurance of adequate safety is accomplished, in part, by requiring the RPP-WTP Contractor to conform to top-level standards and principles that were derived from general nuclear and radiological safety principles that evolved from many years of nuclear facility design, construction, and operation.
- 4.3 Diverse assurance of adequate safety is accomplished by specifying the following:
 - Multiple approaches for controlling radiation doses to workers, co-located workers and the public, including:
 - the radiation dose standards (Table 1)
 - occupational radiation exposure limits in accordance with 10 CFR 835 Operations, Accident, and Worker Accident Risk Goals
 - NESHAP limits on effluent releases during normal operations
 - ALARA and design action thresholds.
 - Multiple requirements for engineering or administrative controls, each of which is adequate to or contributes to prevent hazardous situations that could potentially result in unacceptable consequences to workers, co-located workers, or members of the public or provides sufficient mitigation of event consequences to maintain consequences within limits, including requirements for the following:

⁵³ Ibid., Section 4.2.4.1.

- Confinement system designed to retain radioactive and hazardous material for the entire range of events considered in the design basis
 - Use of automatic systems to achieve and maintain a safe state
 - Primary boundaries for radioactive and hazardous materials designed with margin to withstand worst-case service conditions and with adequate corrosion/erosion allowances for the design life of the facility
 - Important-to-safety equipment designed and constructed to allow adequate testing and inspection
- Defense-in-depth requirements that contribute to accident prevention or mitigation, including:
 - human factors for design
 - operating limits (Technical Safety Requirements)
 - quality assurance/quality control requirements
 - formal configuration management
 - the use of proven designs and engineering practices
 - operating and emergency operating procedures
 - emergency preparedness/emergency plans
 - an unreviewed safety question determination process.

4.4 The radiation dose standards (Table 1) are an acceptable and reasonable basis for evaluating postulated accident consequences, normal radioactive material releases, and confirming the acceptability of preferred control strategies because:

- The dose standards were derived from dose standards specified in NRC regulations for non-reactor nuclear facilities, DOE guidelines either in use or proposed for use throughout the DOE complex, and the Department of Energy Radiological Control Manual. The DOE guidelines used are documented in EH-12-94-01. The dose standards are consistent with DOE Nuclear Safety Policy (e.g., Secretary of Energy Notice SEN-35-91). Although draft standard DOE-STD-3005 existed when the RPP-WTP radiation dose standards were developed, it was not used as a basis/reference for the dose standards.
- The assignment of severity levels in accordance with Table 2, based on the results of conservative hazard analyses, ensures that the radiological exposures to workers, co-located workers, and members of the public due to potential facility off-normal or accident events are well within the thresholds established by the radiation dose standards (Table 1). This is true because of the following:
 - The severity level so established dictates the target frequency for the mitigated event; thus, setting the requirements for the reliability and robustness (i.e., conditional failure probabilities) of the preventive and/or mitigative control strategies implemented into the facility design

(Table 3).⁵⁴

- Accident consequences are evaluated 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.
- The effect of the above is to move event consequences or frequencies away from the thresholds of the radiation dose standards and towards the center of the frequency bins.

While the radiation dose standards provide an effective tool for the RPP-WTP Contractor to determine the necessary preventive and mitigative control strategies to protect against the hazards associated with the RPP-WTP design and operations, including potential accidents, they are only one element of the program intended to ensure the health and safety of workers, co-located workers, and the public. Only through the RPP-WTP Contractor's implementation of the comprehensive radiological, nuclear, and process safety program discussed in Section 3, and RU verification of adequate implementation through the review and approval of required regulatory submittals, inspections, design review oversight, etc., is adequate safety of the workers and public ensured. Dropping any single element of the program, e.g., the radiation dose standards, reduces the robustness of the program.

Recognizing that, while the design and operational objective is to prevent the accidental irradiation of the public or workers, the potential for equipment failures and/or operator errors of commission or omission exists and it is therefore necessary to account for these failures and errors in the facility hazards and accident analyses.

- 4.5 The radiation dose standards established for RPP-WTP are unique to the project and are not necessarily applicable elsewhere in the DOE complex. Some of the dose standards were developed by BNFL Inc. (BNFL) following the RPP-WTP contract-based, integrated safety management process and approved by the RU. Different dose standards were selected by Lockheed Martin Advanced Energy Systems (a previous program contractor) using the same process, and were approved by the RU.
- 4.6 The technical safety objectives, if properly implemented by the RPP-WTP Contractor within the framework of the ISM program, provide additional assurance that the release of radioactive material from the RPP-WTP facility will be precluded or minimized.
- 4.7 The RU limits the number and kind of anticipated or unlikely events that could occur per year by verifying that the calculated facility risk is within of risk goals established for the

⁵⁴ As an example, consider a potential hazardous situation which is determined to result in an unmitigated dose greater than 5 rem but less than or equal to 25 rem to a worker or co-located worker. As can be seen from the radiation dose standards (Table 2), workers and co-located workers may receive up to 25 rem from an Unlikely Event (10^{-2} to 10^{-4} events per year). However, the Safety Requirements Document required accident analysis process requires events having unmitigated dose consequences of 5 to 25 rem to have sufficient preventive and/or mitigative control strategies (SSC) to occur less frequently than once every ten thousand years (Tables 1 and 3).

project. These risk goals limit the collective risk of normal operations and potential accident events for the RPP-WTP facility.

To demonstrate conformance with the risk goals the risk assessment performed by the RPP-WTP Contractor should consider the risk of all events including those that are less frequent than 10^{-6} per year, to the extent that information is available to estimate the risk.⁵⁵

4.8 An acceptable process has been implemented, within the framework of the integrated safety management program, to determine the important-to-safety structures, system, and components, as follows:⁵⁶

- RPP-WTP SSC are classified as important to safety if they are necessary to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public.
- Important-to-safety SSC classifications used for RPP-WTP are further classified as either Safety Design Class or Safety Design Significant.
- Safety Design Class includes those SSC needed to prevent or mitigate accidents that could exceed public or worker radiological or chemical exposure standards and those needed to prevent criticality. This set of SSC includes both the front line and support systems needed to meet these exposure standards or to prevent criticality.
- Safety Design Significant includes those SSC needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation, and SSC that place frequent demands on, or adversely affect the function of, Safety Design Class SSC if they fail or malfunction.

4.9 The RPP-WTP Contractor is committed by the Safety Requirements Document to prepare TSRs, as necessary, and to operate the facility in accordance with the TSRs. The TSRs will be based on the facility accident analysis included in the Final Safety Analysis Report (FSAR) and specific commitments made in the FSAR relative to:

- Process variables, design features, and operating restrictions that are the initial conditions for accident analysis that relate to worker and public safety.
- SSC that must function to prevent or mitigate anticipated, unlikely, and extremely unlikely events to achieve compliance to the worker and public radiological exposure standards (Table 1).

⁵⁵ RL/REG-2000-08, Section 5.0.

⁵⁶ Note that these definitions for Safety Design Class and Safety Design Significant are somewhat unique to the RPP-WTP in comparison to other DOE facilities.

Administrative controls and management systems may have TSRs, but for defense-in-depth only. They receive no numerical credit in accident analysis.

- 4.10 Defense-in-depth requirements have been defined for consideration in the design and operation of RPP-WTP for the purpose of providing robustness in the level of safety designed into the facility.
- 4.11 The RPP-WTP Contractor has implemented a comprehensive ISM program to protect the health and safety of workers and the public. The program conservatively analyzes the consequences associated with unmitigated events having frequencies of occurrence as low as 10^{-6} per year.
- 4.12 There are 86 requirements statements contained within DOE/RL-96-0006 to which the RPP-WTP Contractor is obliged to conform. In addition, the Contractor must institute an integrated safety management program, follow the contract-prescribed process for selection of standards, and comply with applicable rules and laws. It may be possible to reduce the number of requirements statements in DOE/RL-96-0006 without producing an adverse effect on adequate safety. However, a wholesale reduction to a small number is not feasible. Adequate safety is achieved by conformance to a multiplicity and diversity of broad requirements that encompass design, construction, and operations and that include a sufficient recognition of the behavioral factors inherent in QA, ALARA, responsibility and culture.

5.0 REFERENCES

10 CFR 708, "DOE Contractor Employee Protection Program," *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.

29 CFR 1904, "Recording and Reporting Occupational Injuries and Illnesses," *Code of Federal Regulations*, as amended.

29 CFR 1910, "Occupational Safety and Health Standards," *Code of Federal Regulations*, as amended.

29 CFR 1926, "Safety and Health Regulation for Construction," *Code of Federal Regulations*, as amended.

40 CFR 61, "National Emission Standards for Hazardous Air Pollutants," *Code of Federal Regulations*, as amended.

ANSI/ANS-58.9, *Single Failure Criterion for Light Water Reactor Safety-Related Fluid Systems*, American National Standards Institute/American Nuclear Society.

Design Safety Features BNFL Document # RPT-W375-RU00001, Rev. 0, BNFL Inc., Richland Washington, 1999.

DOE/RL-96-0004, *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1996.

DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, Rev. 1, U.S. Department of Energy, Richland Operations Office, 1998.

DOE/RL-96-25, *Policy for Radiological, Nuclear, and Process Safety Regulation of TWRS Privatization Contractors*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1996.

DOE/RL-96-26, *Memorandum of Agreement for the Execution of Radiological, Nuclear, and Process Safety Regulation of TWRS Privatization Contractors*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1996.

Employee Concerns Program, BNFL-5193-ECP-01, Rev. 0, BNFL Inc., Richland, Washington, 1997.

IEEE 379-1994, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, Institute of Electrical and Electronic Engineers, IEEE Power Engineering Society.

INSAG-3, *Basic Safety Principles for Nuclear Power Plants*, International Nuclear Safety Advisory Group, International Atomic Energy Agency.

Integrated Safety Management Plan, BNFL-5193-ISP-01, Rev. 4, BNFL Inc., Richland, Washington, 1998.

Quality Assurance Program and Implementation Plan (QAPIP), BNFL-5193-QAP-01, Rev. 4, BNFL Inc., Richland, Washington, 1998.

Radiation Protection Program for Design (RPP-WTP), BNFL-TWP-SER-003, Rev. 3, BNFL Inc., Richland, Washington, 1999.

RL/REG-97-13, *Regulatory Unit Position on Contractor-Initiated Changes to the Authorization Basis*, Rev. 7, U.S. Department of Energy, Richland Operations Office, 2000.

RL/REG-98-08, *Regulatory Unit Position on Selected Hazards Control Strategy Issues*, Rev. 2, U.S. Department of Energy, Richland Operations Office, 1998.

RL/REG-98-13, *Standards Identification Exercise*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1998.

RL/REG-98-21, *Regulatory Unit Position on Implementing and Assuring Compliance with Integrated Safety Management*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1998.

RL/REG-98-23, *Bases for the Top-Level Standards and Principles and Glossary Definitions*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1998.

RL/REG-99-16, *Regulatory Unit Position on the Selection of Design Standards*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1999.

RL/REG-99-18, *Regulatory Unit Position on Assessment of the Contractor's Integrated Safety Management Program as Described in the Integrated Safety Management Plan*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 1999.

RL/REG-2000-07, *Regulatory Position on Acceptability of the TWRS-Privatization Dose Standards for Unlikely and Extremely unlikely Events*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 2000.

RL/REG-2000-08, *Regulatory Position on Conformance with Risk Goals in DOE/RL-96-0006*, Rev. 0, U.S. Department of Energy, Richland Operations Office, 2000.

Safety Requirements Document (SRD), BNFL-5193-SRD-01, Volumes I and II, Rev. 2, BNFL Inc., Richland, Washington, 1998.

Tank Waste Remediation Privatization Project Design Safety Features, RPT-W375-RU00001, BNFL Inc., Richland, Washington, 1999.

6.0 LIST OF TERMS

AIHA	American Industrial Hygiene Association
ALARA	as low as reasonably achievable
BNFL	BNFL Inc.
CONOPS	Conduct of Operations
DBE	Design Basis Event
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
ECP	Employee Concerns Program
EPA	Environmental Protection Agency
ERPG	Emergency Response Planning Guidelines
FSAR	Final Safety Analysis Report
HAZOP	hazard and operability
ISM	Integrated Safety Management
ISMP	Integrated Safety Management Plan

NESHAP	National Emission Standards for Hazardous Air Pollutants
NPR	New Production Reactor
NRC	U.S. Nuclear Regulatory Commission
PSAR	Preliminary Safety Analysis Report
QA	quality assurance
QAPIP	Quality Assurance Program and Implementation Plan
RO	Regulatory Official
RU	Regulatory Unit
SL	severity level
SRD	Safety Requirements Document
SSC	structures, systems, and components
TSR	Technical Safety Requirement
RAMI	Reliability, Availability, Maintainability, and Inspectability
RPP-WTP	River Protection Project Waste Treatment Plant
USQ	Unreviewed Safety Question

This page intentionally left blank.