U.S. Department of Energy
Office of River Protection
Mr. R. J. Schepens
Manager
P.O. Box 450, MSIN H6-60
Richland, Washington 99352

CCN: 040382

Dear Mr. Schepens:

CONTRACT NO. DE-AC27-01RV14136 – TRANSMITTAL FOR INFORMATION– AUTHORIZATION BASIS CHANGE NOTICE 24590-WTP-ABCN-ESH-02-030, REVISION 0, *CHANGE IN DESIGN CRITERIA DATABASE SOFTWARE (ISMP SECTION 1.3.16.6)*

Bechtel National, Inc. (BNI) is submitting Authorization Basis Change Notice (ABCN), 24590-WTP-ABCN-ESH-02-030, Revision 0, to the U.S. Department of Energy, Office of River Protection and the Office of Safety Regulation (OSR) for information (attached). This ABCN deletes the word "Access ©" from Section 1.3.16.6 of the Integrated Safety Management Plan as the prescribed software product for the Design Criteria Database.

An electronic copy of ABCN 24590-WTP-ABCN-ESH-02-030, Revision 0, is provided for the OSR's information and use.

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

Very truly yours,

R. F. Naventi
Project Manager

TB/slr

Attachment: Authorization Basis Change Notice (ABCN), 24590-WTP-ABCN-ESH-02-030, Revision 0, plus attachments

cc: Name (ALPHABETIZE)	Organization	MSIN
Barr, R. C. w/a (1 hard copy and 1 electronic copy)	OSR	H6-60
Barrett, M. K. w/a	ORP	H6-60
Beranek, F. w/o	WTP	MS6-P1
Betts, J. P. w/o	WTP	MS4-A1
Dickey, R. L. w/a	WTP	MS6-R1
DOE Correspondence Control w/a	ORP	H6-60
Elliott, W. T.	WTP	MS4-C1
Erickson, L. w/a	ORP	H6-60
Gibson, K. D. w/a	WTP	MS6-R1
Naventi, R. F. w/o	WTP	MS4-A1
Ollero, J. E. w/o	ORP	H6-60
PDC w/a	WTP	MS5-K1
QA Project Files w/a	WTP	MS4-A2
Ryan, T. B. w/a	WTP	MS6-R1
Spezialetti, W. R. w/o	WTP	MS6-P1
Struthers, D. J. w/o	ORP	H6-60
Swailes, J. H. w/a	ORP	H6-60
Taylor, W. J. w/a	ORP	H6-60
Veirup, A. R. w/o	WTP	MS4-A1

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-02-030 Revision 0

ABCN Title Change in Design Criteria Database Software (ISMP Section 1.3.16.6)

I. ABCN Review and Approval Signatures

A. ABCN Preparation

	Print/Type Name	Signature	Date
Preparer:	W. T. Elliott		
Reviewer:	Jim Hummer		

B. Required Reviewers

Review Required? *For each person checked, that signature block must be completed.*

Review Required?	Role	Print/Type Name	Signature	Date
☒	ES&H Manager	Fred Beranek		
☒	QA Manager	George Shell		
☒	PSC Chair	Bill Poulson		
☐	Commissioning/Training Manager			
☒	Engineering Manager	Fred Marsh		
☐	Construction Manager			
☐	Area Project Manager			
☐	Research & Technology Manager			
☐	PMT Chair			
☒	ISMP Document Custodian	Rodger Dickey		
☐	Other Affected Organization			
☐	Other Affected Organization			

C. ABCN Approval

	Print/Type Name	Signature	Date
WTP Project Manager	Ronald F. Naventi		

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-02-030 Revision 0

ABCN Title Change in Design Criteria Database Software ISMP Section 1.3.16.6

II. Description of the Proposed Change to the Authorization Basis

D. Affected AB Documents:

Title	Document Number	Revision
Integrated Safety Management Plan	24590-WTP-ISMP-ESH-01-001	1

Decision to Deviate ☐ Yes ☒ No

If yes, DTD Number/Revision N/A DTD Closure Date:

Initiating Document Number/Revision N/A N/A

E. Describe the proposed changes to the Authorization Basis Documents:

Change Section 1.3.16.6 of the ISMP as shown in Attachment 1 to remove the reference to Microsoft Access© as the software product that is used for the Design Criteria Database (DCD).

F. List associated ABCNs and AB documents, if any:

N/A

G. Explain why the change is needed:

The change is necessary to allow flexibility in choosing the appropriate software for the DCD. This change removes the prescription of a particular software, which in turn prevents obsolescence as the project matures, corporate standards change, and software support availability from industry changes over time.

H. List the implementation activities and the projected completion dates:

Activity	Date
Inform DOE that AB has been revised and formally transmit electronic version	30 days or less after PM approval
Distribute revised controlled copy pages / update WTP Library	30 days after PM approval
Revise the following implementing documents:	

	Documents	Describe extent of revisions	Date
1	N/A	N/A	
2			

	Describe other activities:	Date
1	N/A	

ABCN Number 24590-WTP-ABCN-ESH-02-030 Revision 0

ABCN Title Change in Design Criteria Database Software ISMP Section 1.3.16.6

Describe other activities:	**Date**
2	

III. Evaluation of the Proposed Change

I. Is DOE approval required? Answer questions for Administrative Control changes OR Facility changes, not both.

For an <u>Administrative Control</u> change:	**Yes**	**No**
1. Does the revision involve the deletion or modification of a standard previously identified or established in the SRD?	☐	☒

Explain:

The SRD does not identify or establish a standard for the type of database that will be used as the DCD. A text search of the SRD was performed using the words “access”, design criteria database”, and “DCD” with no relevant hits returned. No discussion of and Access database or the design criteria database was found in the SRD. Additionally, Appendix A “Implementing Standard for Safety Standards and Requirements Identification” from Volume II of the SRD, which addresses requirements identification, was reviewed for potentially related standards. No standards were found which indicate that an Access© database is specified for the DCD. Therefore the revision does not involve the deletion or modification of a standard previously identified or established in the SRD.

	Yes	**No**
2. Does the revision result in a reduction in commitment currently described in the AB?	☐	☒

Explain:

The change allows a different software tool to be used for maintaining the design criteria in the DCD. The commitment to compile design criteria in a database with stated capabilities is not changed. By removing the reference to one particular software product, the change will allow selection of the most appropriate software tool to house the DCD. The ISMP section being changed by this ABCN is the only place in the AB documents that identifies Microsoft Access© as the DCD software. The change in software products does not reduce the commitment to maintain the design criteria in a format with user capability to search and locate applicable criteria.

	Yes	**No**
3. Does the revision result in a reduction in the effectiveness of any procedure, program, or plan described in the AB?	☐	☒

Explain:

The change allows a different software program to be used for the DCD. As discussed above in III, I, 2, the effectiveness of the ability of the DCD to provide desired results will not be diminished by allowing different software to be used. Since the change involves allowing the use of different software, and does not affect the program for managing design criteria, then it does not result in a reduction in the effectiveness of any procedure, program or plan described in the AB.

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-02-030 Revision 0

ABCN Title Change in Design Criteria Database Software ISMP Section 1.3.16.6

For a <u>Facility (technical)</u> change: **Yes** **No**

1. Does the revision involve the deletion or modification of a standard previously identified or established in the SRD? ☐ ☐

   Explain:

   N/A

2. Does the revision create a new Design Basis Event (DBE)? ☐ ☐

   Explain:

   N/A

3. Does the revision result in the more than a minimal increase in the frequency or consequence of an analyzed DBE as described in the Safety Analysis Report? ☐ ☐

   Explain:

   N/A

4. Does the revision result in more than a minimal decrease in the Safety Functions of important-to-safety SSCs or change how a Safety Design Class SSC meets its respective safety function? ☐ ☐

   Explain:

   N/A

J. Complete the safety evaluation by describing how the revision to the AB:

1. will continue to comply with all applicable laws and regulations (e.g., 10 CFR 830, 10 CFR 835), conform to top-level safety standards (e.g., DOE/RL-96-0006), and provide adequate safety.

   The change consists of providing flexibility in the choice of software used for the DCD. There is no change to actual operations as a result of this AB change that will impact compliance with applicable laws and regulations, conformance to top-level safety standards or provisions for adequate safety.

2. will continue to conform to the contract requirements associated with the authorization basis document(s) affected by the revision.

   Utilizing a different software product for the DCD does not alter the content or format of the ISMP in a manner that results in a lack of conformance to the original submittal requirements. Therefore the authorization basis document affected by this revision will continue to conform to contract requirements.

3. will not result in inconsistencies with other commitments and descriptions contained in portions of the authorization basis or an authorization agreement not being revised.

   Since the software product used for the DCD is not specified or discussed in any other AB document, nor any other place in the ISMP, other than the section being changed, then the change cannot result in inconsistencies with other commitments and descriptions contained in portions of the authorization agreement not being revised.

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-02-030 Revision 0

ABCN Title Change in Design Criteria Database Software ISMP Section 1.3.16.6

K. Justification of the Proposed Change

If the change requires DOE approval, provide a justification that demonstrates that the proposed change is safe.

N/A

L. Certification of Continued SRD Adequacy

Based on evaluations from III.I, if either question III.I.1 is marked "Yes", Project Manager certification is required. The Project Manager's signature certifies that the revised SRD continues to identify a set of standards that provides adequate safety, complies with WTP applicable laws and regulations, and conforms with top-level safety standards and principles. This certification is based on adherence to the DOE/RL-96-0004 standards identification process and successful completion of review and confirmation by the PSC.

WTP Project Manager:	NA		
	Print/Type Name	*Signature*	*Date*

M. List of Attachments

1. Proposed changes to Integrated Management Safety Plan (ISMP)

24590-WTP-ABCN-ESH-02-030 Rev 0

Attachment 1

24590-WTP-ABCN-ESH-02-030, Revision 0

Document Part	Title	Starting Page	No. of Pages
Section 1.0	Project Safety Approach	1-1	25

# of pages (including cover sheet): 26

1.0 Project Safety Approach

The WTP Contractor's safety approach is implemented with the recognition that the defined work for processing and immobilizing Hanford tank waste involves inherent radiological and chemical hazards from which hazardous situations may arise. The WTP Contractor is committed to integrating the development of safety criteria and design requirements, the hazard analysis and accident analysis process, and the facility design to minimize the risk associated with these hazards and hazardous situations. The WTP Contractor accepts responsibility for the safety of the WTP and for adequate protection of the health and safety of the public, worker safety, environmental protection, and compliance with applicable laws and regulations.

This chapter of the Integrated Safety Management Plan (ISMP) provides an overview of the WTP design, construction, and commissioning (DC&C) Contractor (i.e., Bechtel National, Inc. [BNI]) safety approach developed for the River Protection Project – Waste Treatment Plant (WTP). The elements of this approach, through their evolutionary implementation in Part A of the project, form the bases for this ISMP. The ISMP is followed and will be further developed during Part B of the Project for detailed design, construction, operation, and deactivation of the facility.

The Project safety approach is summarized in Section 1.1, "Introduction". The components of the safety approach are described in greater detail in Section 1.2, "Summary". The elements of the safety approach are described in Section 1.3, "Description of the Integrated Safety Management Plan".

1.1 Introduction

The safety management practices outlined in the ISMP have been developed specifically for the Project. The development of these management practices was based on the experience of the Project team at other nuclear facilities in the areas of design, construction, and operation. These practices ensure implementation of the corporate policy that no activities are more important than the health and safety of its workers, contractors, the public, or protection of the environment.

The ISMP documents the process by which laws, regulations, and standards applicable to the nuclear, radiological, and process safety aspects of the Project are incorporated into programs for facility design, construction, operation, and deactivation to ensure adequate safety of workers and the public and protection of the environment. A further role of the ISMP is to demonstrate how practices are in line with the WTP Contractor policies to ensure that the safety culture achieved at other nuclear chemical facilities can be successfully sustained through the different phases of the WTP. At this stage in the project, the ISMP is biased towards the design and construction phase, during which most of the processes described are developed. However, the principles of the ISMP for later stages of the facility life through operation and deactivation and how the design and construction phase will be integrated into these later stages is discussed. The ISMP also describes how the safety management practices will be followed and further developed during Part B of the Project.

Table 1-1~~1~~ BNFL Team Experience Related to the TWRS-P Project (this table has been deleted)

To accomplish its roles, the ISMP describes the following:

1) The facility defined work to process and immobilize Hanford Tank waste in a safe manner (ISMP Section 1.3.1, "Project Initiation")

2) The selection of a safe and proven technology (ISMP Section 3.7, "Proven Engineering Practices")
3) The development and use of the SRD (ISMP Section 1.3.3, "Safety Requirements Document")
   a) To establish the Safety Criteria by which the process hazard analysis (PHA) and accident analysis identify features required for worker and public safety
   b) To identify the design requirements that, when implemented, ensure that prevention and mitigation controls will perform their specified safety functions
4) The use of PHA to identify the full range of potential radiological and chemical hazards and hazardous situations (ISMP Section 1.3.4, "Process Hazards Analysis")
5) The accident analyses performed to identify engineered and administrative controls required for worker and public safety (ISMP Section 1.3.6, "Accident Analysis")
6) The iteration of the PHA, accident analyses, and design to ensure an adequate level of safety for the workers and the public (ISMP Sections 1.3.7, "Acceptable Level of Public Safety" and 1.3.8, "Acceptable Level of Worker Safety")
7) The development of the technical safety requirements, if required, that are based on:
   a) A process variable, design feature, or operating restriction that is an initial condition (i.e., the assumed facility state) for an accident analysis
   b) Structures, systems, and components that must function to maintain compliance with public and worker radiological and chemical exposure standards
8) The development of procedures and training to achieve and maintain the required administrative controls (ISMP Sections 1.3.12, "Training" and 1.3.13, "Procedures")
9) The development of an emergency preparedness program and implementing procedures (ISMP, Section 1.3.18, "Emergency Planning")
10) The assignment of design, construction, and operational roles and responsibilities and the use of assessments to ensure the necessary attributes of the ISMP are effectively accomplished (ISMP, Chapters 10.0, "Assessments", and 11.0, "Organizational Roles, Responsibilities, and Authorities")

Chapter 1.0 of the ISMP presents the BNI safety approach. Chapters 2.0 through 11.0 are formatted to correspond to the attributes included in RL/REG-97-07, *Guidance for the Review of TWRS Privatization Contractor Integrated Safety Management Plan Submittal Package* (DOE-RL 1997).

Throughout the ISMP, lists of items are numbered for the convenience of the reviewers in referring to individual items. The numbering is not an indication of the importance or sequence of the items.

Chapter 12.0, "Definitions", contains the definitions of some of the terms, phrases, or documents that are found throughout the ISMP. When used unmodified in the ISMP, "worker" refers to the facility and collocated worker, both individually and collectively.

Within this document, the *Safety Requirements Document* (SRD) (BNI 2001b and BNI 2001c), *Hazard Analysis Report* (HAR) (BNFL 1997b), *Quality Assurance Program* (QAP) (BNFL 1997a, BNFL 1998c), *Quality Assurance Manual* (QAM) (BNI 2001), and *Initial Safety Analysis Report* (ISAR) (BNI 2001d and 2001e), are cited using acronyms. Full reference information for these documents appears in Chapter 13.0, "References".

1.2 Summary

The Project safety approach is implemented with the recognition that the defined work of processing and immobilizing Hanford tank waste involves inherent radiological and chemical hazards from which hazardous situations may arise. The Project is integrating the development of Safety Criteria, design requirements, the hazard analysis and accident analysis processes, and the facility design to minimize the risk associated with these hazards and hazardous situations. The elements of this approach, through their evolutionary implementation in Part A of the Project, form the bases for this ISMP.

The safety approach for the Project is based on applying best industry practices and cost-effective processes that come from successful and safe operation in the commercial nuclear environment and the chemical process industry. The purpose of the safety approach is to achieve the following objectives.

1) Ensure an adequate level of safety at the facility for the workers and the public.
2) Comply with applicable laws and regulations.
3) Conform to top-level safety standards and principles stipulated by the U.S. Department of Energy (DOE-RL 1996b).

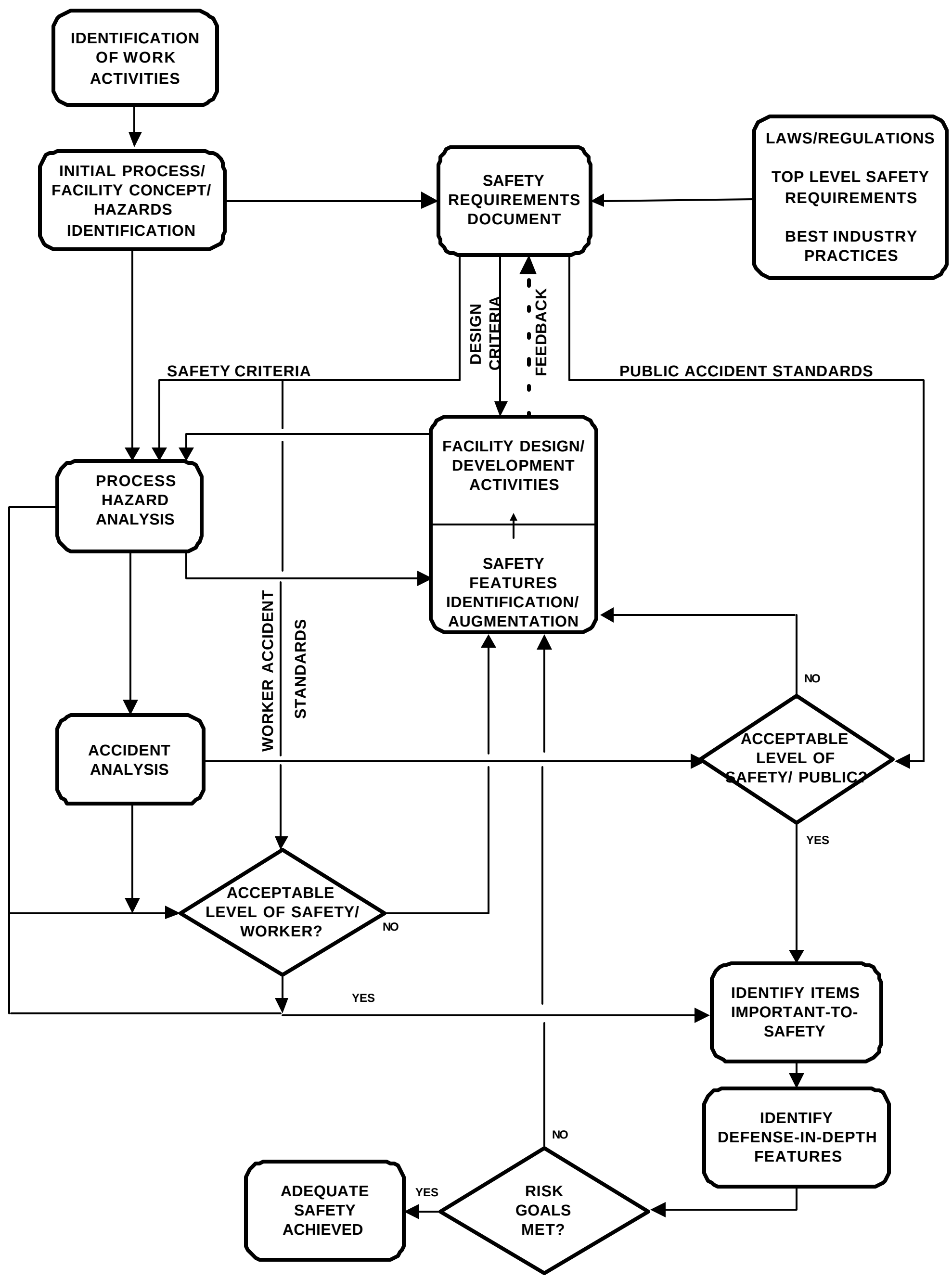
A diagram of the Project safety approach is presented in Figure 1-1. The safety approach begins with the definition of the work to be performed and continues with the development of the conceptual process flow diagrams (PFD) and other facility design information required to accomplish the defined work. The PFDs and design development give consideration to the types of work to be accomplished, the hazards identified for similar facilities, and the methods by which these hazards were previously eliminated or controlled for similar facilities. This conceptual information is used to identify appropriate hazards-based standards and initiate the development of the SRD.

The identification of hazards and hazardous situations helps to characterize the hazardous situations as those that may require prevention or mitigation. The identification and characterization of the hazards and hazardous situations establish a basis for describing approaches and measures to control the hazards. Safety Criteria are then developed that document the set of standards and requirements necessary to ensure implementation of the necessary hazard control strategies. These Safety Criteria are documented in the SRD and are based on applicable laws and regulations, the U.S. Department of Energy's (DOE) top-level safety requirements, and best industry practices. The SRD provides Safety Criteria to the PHA by which an initial assessment of the adequacy of the design is made.

As accident prevention and mitigation safety features are identified in the PHA, the resulting facility design impacts are fed back to the SRD process, as required, for further development of more detailed Safety Criteria and design requirements to ensure all safety features provide their specified safety functions.

As the PHA, PFDs, and facility design mature, accident analyses are performed to confirm judgements made during the PHA and to further characterize the accident scenarios to demonstrate compliance with radiological and chemical exposure standards for accidents. Additional protection for workers is identified by the PHA, the accident analyses, and the application, as appropriate, of Process Safety Management (PSM) required by 29 CFR 1910.110.

Figure 1-11 Project Safety Approach



Significant features of the Project safety approach are described as follows.

1) The approach continually integrates hazard identification, SRD development, design development, and accident analysis throughout the facility design, construction, operation, and deactivation phases.

2) The approach uses the best industry practices that include PHA, a rigorous design process based on a set of credible accidents and a defense-in-depth philosophy, and verification of the level of facility safety through accident analysis and validation of requirements implementation.
3) The PHA identifies and evaluates the significance of potentially hazardous situations. For each identified event, a defense-in-depth approach applies a level of protection in terms of engineered features and administrative controls that is commensurate with the severity of the unmitigated event. The hazards evaluation techniques satisfy the requirements of a hazards analysis process established by the American Institute of Chemical Engineers (AIChE 1992).
4) A conservative approach to accident consequence analysis is used in terms of input assumptions, boundary conditions, and modeling techniques. As the process and facility design mature, the modeling is refined to eliminate unnecessary conservatism. This strategy is consistent with risk-based approaches that allow the use of uncertainty analysis to better identify the impact of assumptions and state of knowledge on results from the safety analyses.
5) The safety approach documents how the identification of the engineered and administrative controls credited for public and worker safety and facility Safety Criteria is accomplished.

This approach to safety analysis is similar to that described in draft NUREG 1513, *Integrated Safety Analysis Guidance Document,* (NRC 1994) published by the U.S. Nuclear Regulatory Commission (NRC).

1.3 Description of the Integrated Safety Management Plan

Each of the elements of the safety approach are described in detail in the following sections.

1.3.1 Project Initiation

The Project safety approach began with a discussion to aid in understanding of the work to be accomplished and the development of the conceptual design of the processes and facility to accomplish this work. The development of the conceptual design considered the work to be performed, hazards and hazardous situations identified for similar facilities, and the methods to eliminate or control these hazards and hazardous situations. Early in the development of the conceptual design, hazards identification and evaluation techniques appropriate for the preliminary nature of the process and facility design were selected and applied.

1.3.2 Laws/Regulations/Top-Level Safety Requirements/Best Industry Practices

Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors, DOE/RL-96-0006 (DOE-RL 1996b) provides a set of top-level radiological, nuclear, and process safety standards and principles prescribed by DOE for accomplishing the required level of safety for the WTP. This document is used as one resource for the development of the SRD. Included in DOE/RL-96-0006 are radiological exposure and risk standards for evaluation of normal and offnormal events. Additional resources for the identification of standards were derived from the U.S. and United Kingdom (UK) commercial nuclear and chemical industries. The identification of the remaining requirements is described in the following section.

1.3.3 Safety Requirements

The SRD defines the Safety Criteria and the design requirements (implementing codes and standards) necessary to protect the public and workers from radiological, nuclear, and process hazards and hazardous situations. The Safety Criteria and codes and standards of the SRD are applied to the WTP. The SRD, as well as the ISMP, applies to Project contractors. By application of the SRD and ISMP to all Project activities, a consistent project-wide approach is applied to Environmental, Safety, and Health (ES&H) matters. The hazards and hazardous situations at the facility will change significantly throughout the construction, operation, and deactivation phases of the Project. The SRD was developed by an iterative process that will continue as the design matures through the construction, commissioning, operation, and deactivation of the facility. The development involved identifying the work to be performed, identifying hazards and hazardous situations of the facility operation by the PHA and accident analyses, reviewing of pertinent regulations and industry practices, and identifying engineered and administrative controls.

Once the work activity was identified for the Project and the hazards associated with this work determined, the Safety Criteria were defined by the requirements necessary to ensure protection of the public and workers from radiological, nuclear, and process hazards. The Safety Criteria are based on the following:

1) Mandated regulatory requirements (statutory and contractual; including those identified as top-level safety requirements [standards and principles]) and equivalent requirements
2) Requirements and guidance documents deemed relevant to waste management facilities such as this Project
3) Best industry practices from the government, commercial nuclear, and chemical industries

The engineered and administrative controls necessary to eliminate and control hazards and hazardous situations are established via the PHA, the accident analysis, and the necessary level of protection required to satisfy the SRD Safety Criteria. Once the controls are selected, the SRD identifies the implementing codes and standards necessary to ensure that engineered and administrative controls are properly designed, implemented, and maintained. The requirements, guidance documents, and practices are incorporated into the SRD, tailored toward applicability to WTP operations, the control of hazards, and the adequacy to protect public and worker health and safety. These codes and standards are used by the appropriate organizations to ensure that the design, construction, testing, and maintenance of Important-to-Safety SSCs are such that they can perform their specified public and worker safety functions when required. Additional detail on the SRD and definition of Important-to-Safety is provided in ISMP Section 4.1, “Safety Management Processes” and Section 1.3.10, “Classification of Structures, Systems, and Components”.

1.3.4 Process Hazards Analysis

The PHA process is a systematic team-based approach used to identify and analyze the significance of potentially hazardous situations associated with the operation and maintenance of the WTP. Other hazardous situations unique to the deactivation phase will be identified near the end of waste processing operations. The PHA process includes preliminary hazard analysis and Hazard and Operability (HAZOP) Analysis. The process is enhanced by the experience gained by the Project team from similar analyses performed at similar facilities. The PHA is performed to ensure the facility is designed to provide accident prevention and mitigation controls as required to meet safety criteria established for the protection of the public and workers. The PHA team includes members experienced in the engineering design and operation of the chemical process being evaluated and at least one member knowledgeable in the specific PHA methodology being used. The results of the PHA are also strengthened by the use of the operational and maintenance experience of the team members to compliment the design process. Specifically, the goals of PHA are to

1) Identify hazards and potential hazardous situations associated with a process or activity
2) Identify features in the design or operation of the facility that could lead to accidents
3) Assist designers in identifying the need for design features to eliminate or control hazards and hazardous situations
4) Identify principal operability concerns to assist designers in eliminating or minimizing the associated risk

The focus of the analysis is on process safety issues, such as the acute effects of unplanned radiological and chemical releases on the public or workers. The PHA supplements the more traditional industrial health and safety activities that consider, for example, protection against slips or falls, use of personal protective equipment, and monitoring for employee exposures. Additional detail on the PHA is provided in ISMP Section 5.5, "Process Hazards Analysis".

1.3.5 Facility Design/Development Activities and Safety Features Identification

The PHA and the accident analyses identify the need for accident prevention and mitigation controls to satisfy the SRD Safety Criteria. There will be differences between the prevention and mitigation techniques needed during facility operation and those needed during the deactivation process. Both sets of needs are communicated to the design groups for the selection of the most effective and efficient means of achieving the required controls. In the selection of required controls, preference is given to accident prevention over mitigation and engineered features over administrative controls. Preference is also given to passive engineered features over active engineered features (ISMP Section 3.7, "Proven Engineering Practices"). Reliance on human intervention would be used only when reliance on other means of eliminating or mitigating the hazardous situation cannot be used. The features identified are maintained or changed, as needed, as the facility moves from operation to deactivation. Control of the features is discussed in more detail in ISMP Section 3.5, "Quality Assurance Program (QAP)", Section 1.3.16, "Configuration Management", and Section 5.3, "Configuration Management".

1.3.6 Accident Analysis

During the design phase, the set of potential accidents identified by the PHA is carried forward to the accident analysis to identify the need for prevention and mitigation controls required during operation or for deactivation to satisfy the SRD Safety Criteria. The Project team experience with accident analyses for similar facilities is particularly valuable in developing the models for the accident scenarios to be analyzed. Well-established methods that include factors such as the material at risk and the rate and duration of the release of hazardous material are used in the determinations of the source terms (NRC 1988; DOE 1994).

Evaluating potential accidents involves the following tasks:

1) Separating the lower-risk accidents adequately addressed by the PHA from the higher-risk accidents that warrant quantitative analysis to confirm risk acceptance guidelines are satisfied
2) Grouping the accidents based on considerations such as the location of the accident, the phenomena involved, the accident type, and the nature of the hazardous material at risk

3) Calculating the radionuclide or chemical release from the facility and the impact of the release on the facility operators whose actions are credited to maintain the public and workers radiological and chemical exposures within defined standards

1.3.7 Acceptable Level of Public Safety

During the facility design evolution, a consequence analysis is performed for each accident involving a radionuclide or chemical release. For those accidents that involve a radionuclide release, the calculated exposures are compared to the radiological exposure standards of Table 1-2 to determine the need for accident prevention or mitigation features credited for public safety. For chemical release, the projected exposure is compared to the standards of SRD Safety Criterion 2.0-2. If the radiological or chemical release standards are not satisfied, the need for engineered or administrative controls to prevent or limit the release is addressed. These features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention or mitigation of accidents. Features credited for satisfying the public radiological exposure standards of Table 1-2 and chemical release exposure standards of SRD Safety Criterion 2.0-2 are classified as Safety Design Class (which is a subset of Important-to-Safety as discussed in Section 1.3.10, "Classification of Structures, Systems, and Components). The location of the public (i.e., offsite receptor) for the purpose of establishing compliance with Table 1-2 and the chemical release standard, is established at the most limiting exposure location along the near exposure bank of the Columbia River, Highway 240, and a southern boundary as shown in Figure 1-2. If credit is taken for operator action to satisfy the public radiological exposure standards of Table 1-2, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem total effective dose equivalent (TEDE), 30 rem thyroid, and 30 rem beta skin for the duration of the accident. In the event operator action is not required, other than immediate actions required to place the facility operation into a safe state, then the worker exposure standards of Table 1-2 apply. If credit is taken for operator action to satisfy public chemical exposure to the standards specified in SRD Safety Criterion 2.0-2, provisions are made so that the operator exposure does not exceed the standard specified in SRD Safety Criterion 4.3-7.

Table 1-2~~2~~ Radiological Exposure Standards Above Normal Background

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Normal Events: Events that occur regularly in the course of facility operation (e.g., normal facility operations); including routine and preventative maintenance activities.	>0.1	Normal modes of operating facility systems should provide adequate protection of health and safety.	5 rem/yr 50 rem/yr any organ, skin, or extremity 15 rem/yr lens of eye 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b) (1)	5 rem/yr 1.0 rem/yr ALARA design objective per 10 CFR 835.1002(b) (1)	10 mrem/yr (airborne pathway) 100 mrem/yr (all sources) 100 mrem/yr (public in the controlled area) 25 mrem/yr (radioactive waste)
Anticipated Events: Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	10^{-2}<f10^{-1}	The facility should be capable of returning to operation without extensive corrective action or repair.	5 rem/event (2, 3) 1.0 rem/event design action threshold (4)	5 rem/event (2, 3) 1.0 rem/event design action threshold (4)	100 mrem/event (3)

Table 1-22 Radiological Exposure Standards Above Normal Background

Description	Estimated Frequency of Occurrence f (yr^{-1})	General Guidelines	Worker	Collocated Worker	Public
Unlikely Events: Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	$10^{-4}<f10^{-2}$	The facility should be capable of 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)
Extremely Unlikely Events: Events that are not expected to occur during the life of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.	$10^{-6}<f10^{-4}$	Facility damage may preclude returning to operation.	25 rem/event (2, 3)	25 rem/event (2, 3)	25 rem/event 5 rem/event target (3) 300 rem/event to thyroid
Location of Receptor			Within the Controlled Area Boundary	The most limiting location at or beyond the Controlled Area Boundary	The most limiting location along the near river bank/Hwy 240/ southern boundary

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

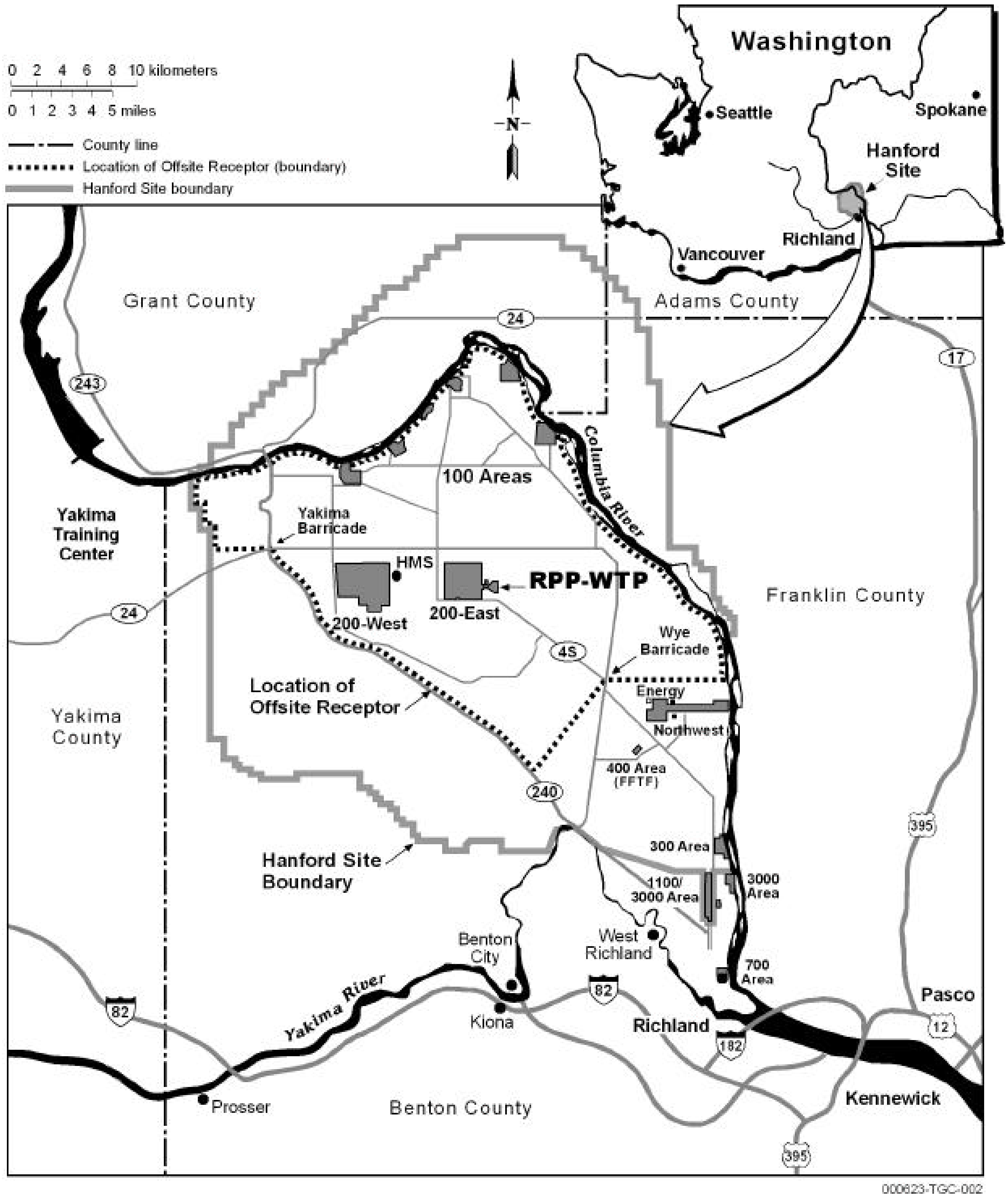
(2) In addition to meeting the listed worker and collocated worker exposure standards for accidents, the Worker Accident Risk Goal is satisfied through the calculation of the risk from accidents with accident prevention and mitigation features added as necessary to meet the goal.

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

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

A conservative approach is applied to accident consequence analysis in terms of input assumptions, boundary conditions, modeling techniques, and compliance with public radiological and chemical release standards. As the process and facility design mature, the analysis is refined to eliminate unnecessary conservatism that may have been applied solely to cover uncertainties in design. This strategy is consistent with a risk-based approach that allows the use of uncertainty analysis to better identify the impact of the assumptions and state of knowledge on results from the safety analysis.

Figure 1-2~~2~~ Location of Public Receptor



1.3.8 Acceptable Level of Worker Safety

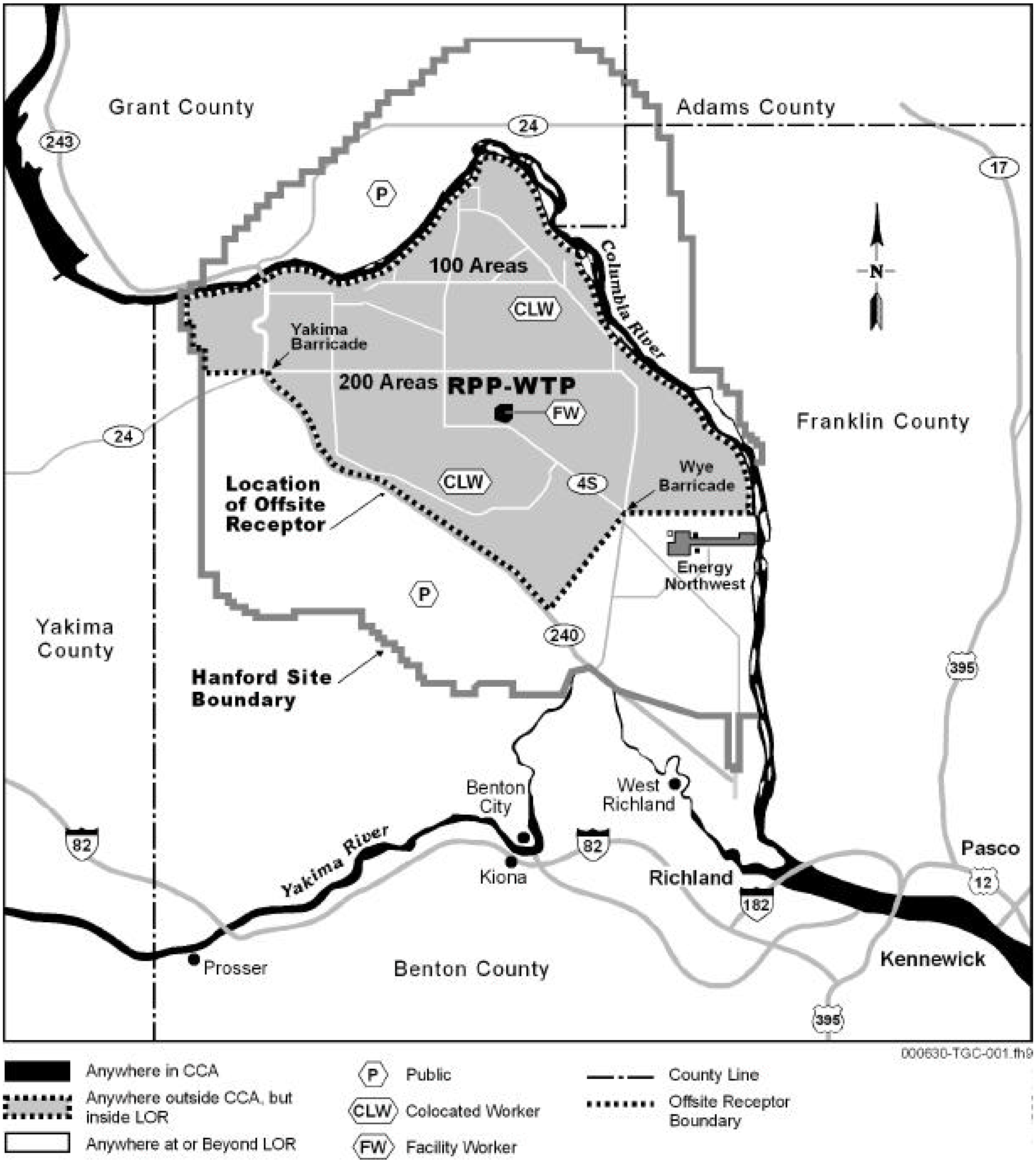
Radiological exposure standards applied to the facility worker and collocated worker are provided in Table 1-2. The location of the workers is shown in Figure 1-3. A 5 rem/event standard is applied to the workers for anticipated events, and a 25 rem/event exposure standard is applied to workers for unlikely and extremely unlikely events. The 25 rem/event standard corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2 x 10^{-2}. For unlikely events (defined in Table 1-2 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of about 2 x 10^{-4}/yr, which is less than the average of the accidental death risk for workers in some of the safest industries, such as retail and wholesale trade, manufacturing, and service (EPA 1991).

Compliance with the 25 rem/event worker standard is established using qualitative methods of the PHA supported, where necessary, by numerical analyses that may include the development of event trees and fault trees or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls to be added to the design are identified. The PHA identifies hazards and operability problems based on the design detail available and experience with similar facilities. Further hazard evaluation takes place in parallel with design development to ensure that safety is built into the design process. Having generated the list of hazards, this list is subject to a further systematic team-based review where a binning process takes place. The binning process is essentially the risk-based categorization of hazards and hazardous situations according to a frequency/consequence matrix.

The 25 rem/event worker standard for unlikely or extremely unlikely events applies to events with frequencies less than 10^{-2}/yr. For those frequencies, the PHA assigns serious and major hazardous situations as either undesirable, acceptable with controls, or acceptable. For a hazardous situation to be acceptable, the situation must have consequences less than 25 rem. Where there is uncertainty concerning the appropriate hazard category to be assigned, the hazard is binned to the higher category to ensure that the accident analysis remains conservative.

For those accidents that involve a radionuclide release, the calculated exposures are compared to the radiological exposure standards of Table 1-2 to determine the need for accident prevention or mitigation features credited for worker safety. For chemical release, the projected exposure is compared to the standards in ERPG-2. If the analysis of radiological or chemical exposures do not confirm the adequacy safety, the need for engineered or administrative controls to prevent or limit the release is addressed. These features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention or mitigation of accidents. Features credited for satisfying the radiological exposure standards of Table 1-2 and chemical release exposure standards of ERPG-2 (AIHA 1988) are classified as Safety Design Class.

Figure 1-33 Location of Facility and Collocated Workers



The worker accident risk goal is stated in DOE/RL-96-0006 as, "The risk, to workers in the vicinity of the Contractor's facility, of fatality from radiological exposure that might result from an accident should not be a significant contribution to the overall occupation risk of fatality to workers" (DOE-RL 1996b, Section 3.1.3). This goal is satisfied by calculating the risk of facility operation to the workers at the WTP. This is a best-estimate analysis based on realistic input and modeling assumptions. In performing this analysis, all SSCs capable of preventing or mitigating the event are considered. The evaluation of the availability and reliability of the SSCs include factors such as failures to start and failures to operate, as well as unavailability resulting from maintenance activities. Accident prevention and mitigation controls are added to the design as necessary to satisfy the worker accident risk goal.

If credit is taken for operator action to satisfy the worker radiological exposure standards of Table 1-2, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent (TEDE), 30 rem thyroid, and 30 rem beta skin for the duration of the accident. In the event operator action is not required, other than immediate actions required to place the facility operation into a safe state, then the worker exposure standards of Table 1-2 apply. If credit is taken for operator action to satisfy worker chemical exposure to the standard specified in SRD Safety Criterion 2.0-2, provisions are made so that the operator exposure does not exceed the standard specified in SRD Safety Criterion 4.3-7.

Additional details on the radiological exposure standards applied to the public and workers are provided in Appendix D of 24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*, which also provides information on the basis for the assumed location of the receptors.

1.3.9 Quality Assurance Program

The quality assurance program (QAP) is an important tool in achieving the goal of the safe operation of the WTP. The QAP defines the organizational structure, functional responsibilities, levels of authority, and interfaces for those managing, performing, and assessing the work to be performed. The Project developed its quality assurance program (QAP) in compliance with the requirements of 10 CFR 830.120, "Quality Assurance Requirements", so the integration of the QAP for the TWRS-P Project began during the initial phases of the project. The QAP document for Part A has been submitted to and approved by the U.S. Department of Energy (DOE) (Sheridan 1997). The QAP document for Part B activities has been submitted to DOE; this version (BNFL 1998c) has been approved by the DOE Regulatory Unit (Gibbs 2000). BNI revised the BNFL/CHG QAP document into a Quality Assurance Manual (QAM). This QAM (BNI 2001) superceded the CHG QAP document (i.e., BNFL-5193-ISP-01, Revision 8) in its entirety.

As a result of early development of the QAP, the PHA, SRD, and HAR were developed in accordance with the requirements in the QAP. The application of the requirements of the QAP continues during design, procurement, construction, commissioning, inspections, operations, maintenance, modifications, and deactivation of the facility. Administrative processes such as training, procedure development, and configuration management are subject to the requirements of the QAP. The QAP is used by the Project team to ensure that all aspects of the integrated safety approach have been implemented for the Project.

The WTP Project QAP document (i.e., BNFL-5193-QAP-01, Revision 8) was restructured to reflect BNI QA program policy, as well as use of NQA-1-1989 (ASME 1989), QARD (DOE 2000), and DOE O 414.1A (DOE 1999), as issued in a *Quality Assurance Manual* (BNI 2001). This QAM serves as the Authorization Basis document for implementation of the Project QA program. The QAP requires periodic assessments of activities, both by management and by knowledgeable, independent personnel, as described in QAM section 18. The conduct of audits to objectively evaluate the effectiveness and proper implementation of the QAM for activities affecting quality of SSCs and surveillances of specific project activities (e.g., process controls, preparation of safety documentation, configuration and document control, and records management) to supplement the compliance audit program are also described in the QAM. The QAM also describes the process of qualifying personnel who perform assessments, audits, and surveillances, as well as documentation of results and review by management.

Performance monitoring is used to verify that the necessary programs, plans, and procedures are functioning to ensure that activities are maintained in compliance with the applicable requirements. The findings of performance monitoring are used to determine if changes are needed to ensure that the high standards of performance expected are achieved.

The QAP ensures that identified corrective actions are implemented and any follow-up actions, such as the performance of a re-audit of a deficient condition, are conducted.

Different aspects of the implementation of the QAP are discussed in the following parts of the ISMP:

1) Chapter 2.0 “Compliance with Laws and Regulations”
2) Section 3.5 “Quality Assurance Program”
3) Section 5.4 “Compliance Audits”
4) Chapter 10.0 “Assessments”

1.3.10 Classification of Structures, Systems, and Components

The design classification process used on the Project provides a consistent, project-wide approach for the classification of the WTP SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs will be revised as necessary.

The design classification system provides assurance to DOE that the defined safety functions of SSCs will perform as intended.

In this system, SSCs are designated as Important-to-Safety in accordance with the definition of this term as provided in *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b).

SSCs defined as Important-to-Safety for the WTP include the following.

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Table 1-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs are designated as Safety Design Class.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs are designated as Safety Design Significant.

The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded. However, additional items also are designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis. These latter items are identified by the results of the HAR.

Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the risk analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

SSCs identified in ISAR Section 4.8, “Controls for Prevention and Mitigation of Accidents” as Design Class I and II are Safety Design Class SSCs. SSCs provided to protect the health and safety of the public and collocated workers usually are considered to also provide adequate protection of the environment. As stated in ISAR Section 4.8, “The selection of engineered and administrative controls is based on the conceptual design of the facility. Additional or different features may be identified during Part B”. The more complete group of Important-to-Safety SSCs will be identified in Part B and provided in the Preliminary Safety Analysis Report (PSAR) as part of the Construction Authorization Request. The PSAR and the Final Safety Analysis Report also will describe SSCs that are not designated as Important-to-Safety. The descriptions of these SSCs will note that they are not classified as Important-to-Safety.

When a SSC is designated as Safety Design Class it has the following attributes:

1) Quality Level 1 (QL-1) is applied to the SSC. The QAP describes the requirements associated with QL-1.
2) For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to

occur and progress such that a public or worker accident exposure standard is exceeded. This requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.

3) The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event. For example, if an earthquake can produce exposures to the public or workers in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed to be DBE-resistant and designated as Seismic Category I for radiological hazards (or Seismic Category III for chemical hazards). However, DBE-resistance is not applied automatically to Safety Design Class SSCs. It is applied only when the earthquake is the initiating event, or when the earthquake could cause the initiating event. A Safety Design Class SSC that does not have a DBE mitigating function is designated as Seismic Category III.

   This natural phenomenon hazard (NPH) design philosophy is used for all severe natural phenomena events (i.e., earthquake, flood, high wind). Therefore, if a Safety Design Class SSC is needed for meeting public or worker exposure standards for a given NPH event, the NPH loads associated with that event are taken from SRD Volume II, Table 4-1, "Natural Phenomena Design Loads for Important-to-Safety SSCs with NPH Safety Functions". All other NPH loads for the Safety Design Class SSC may be taken from SRD Volume II, Table 4-2, "Natural Phenomena Design Loads for SSCs without NPH Safety Functions" in lieu of SRD Table 4-1.

4) General design requirements are applied as identified in Section 4.0 of the SRD for Safety Design Class SSCs. See SRD Safety Criterion 4.1-5 as an example.

5) Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0. For example, SRD Safety Criterion 4.4-5 provides requirements associated with Safety Design Class air treatment systems.

6) Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.

7) Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements (discussed in ISMP Section 4.2.3.4 "Technical Safety Requirements").

When a SSC is classified as Safety Design Significant it is has the following attributes.

1) Quality Level 2 (QL-2) is applied to the SSC. The QAP describes the requirements associated with QL-2.

2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event. If an earthquake can produce exposures to the public or workers in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed DBE-resistant as discussed above. The same NPH loads also are applied to a Safety Design Significant SSC if failure of the item could prevent the Safety Design Class SSC from performing its safety function required as a result of the DBE. Such an SSC is designated Seismic Category II. It should be noted, however, that DBE resistance is not automatically applied to Safety Design Significant SSCs. It is applied only when the earthquake is the initiating event, or when the earthquake could cause the initiating event. A Safety Design Significant SSC that does not have a DBE mitigating function is designated Seismic Category III.

This NPH design philosophy is used for all severe natural phenomena events (i.e., earthquake, flood, high wind). Therefore, if a Safety Design Significant SSC is needed to meet public or worker exposure standards for a given NPH event, the NPH loads associated with that event are taken from SRD Volume II, Table 4-1, "Natural Phenomena Design Loads for Important-to-Safety SSCs with NPH Safety Functions". All other NPH loads for the Safety Design Significant SSC may be taken from SRD Volume II, Table 4-2, "Natural Phenomena Design Loads for SSCs without NPH Safety Functions" in lieu of SRD Table 4-1.

3) General and specific design requirements are applied as identified in Section 4.0 of the SRD for Safety Design Significant SSCs.

4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

1.3.11 Quality Levels

The assignment of Quality Levels (QL) is the method by which the implementation of the graded quality approach discussed in 10 CFR 830.120, "Quality Assurance Requirements" is ensured. Designation of correct quality levels helps to ensure that the appropriate quality assurance requirements are applied to specific WTP SSCs. The quality levels of the Project quality assurance approach and their applications are described in the QAP.

1.3.12 Training

Training serves an important role in the Project by ensuring that the personnel involved with the project have sufficient knowledge to safely fulfill the roles and responsibilities of their assigned tasks. Training has a direct impact on safety during design, construction, operation, and deactivation of the project by:

1) Improving technical ability
2) Enhancing personal skills
3) Increasing awareness of signs of potential hazardous situations in the workplace
4) Increasing personal awareness of the potential impact of actions taken with regard to the safety of the individual, others, and the facility
5) Establishing a safety culture that clearly assigns the responsibility for safety to the individual

During the design and construction phases of the project, the training focus is on the requirements such as design evolution, compliance with regulations and commitments, construction activities, and quality assurance.

Operator training and qualification is of specific importance in the training program. The operator training program is enhanced by the experience of the Project team at other similar facilities and by the information made available during the design phase and the commissioning program. In addition, operation of the demonstration plants provides invaluable training opportunities for the facility operators.

In recognition that different training is required for different assignments, the training plan addresses the assessment of training requirements and responsibilities and the evolution of the training plan required as the project matures. Additional information on training is provided in ISMP Section 3.15 "Training and

Qualification" and Section 4.2.2, "Training and Procedures". The training plan is described in ISAR Section 3.4, "Training and Qualification".

1.3.13 Procedures

Procedures are one tool by which compliance with requirements is ensured during the design, construction, operation, and deactivation of the project. All activities that may affect safety of the public and workers are performed in accordance with step-by-step instruction provided in procedures. The range of activities covered in procedures includes, but is not limited to:

1) Design control
2) Procurement activities
3) Monitoring contractors
4) Identification and resolution of nonconforming conditions
5) Operations and maintenance
6) Emergency plan implementing procedures

There is a defined hierarchy of procedures commensurate with the philosophy used to developed the tailored levels of design classification and quality levels. For example, procedures supporting the implementation of Technical Safety Requirements that are credited for accident prevention or mitigation will have a greater safety significance than procedures supporting maintenance activities on other SSCs. Those procedures, at the highest level, are subject to increased rigor with respect to their development, review, implementation, and change. Increased rigor includes requirements for independent review and approval by qualified and experienced personnel or safety committees. Training emphasizes the importance of the hierarchy as well as the content of the procedures and the requirement to follow procedures to ensure safe and efficient activities.

One category of procedures is the operating procedures. These procedures are developed during the design and construction phase, when more detailed design information is available. The design information, test data, and design requirements are incorporated into the operating procedures. The operating procedures address normal and off-normal facility conditions, process startup and shutdown, and emergency events. The development and control of the operating procedures are summarized in ISMP Section 5.6.1, "Procedure Development", and is addressed in ISAR Section 3.9, "Procedures".

1.3.14 Commissioning

Another integral portion of the safety approach is the commitment to a thorough startup testing program. The program validates that the design, construction, hardware, programs, and personnel are ready to support the safe operation of the facility. The tests performed ensure that the equipment and facility are properly built and will operate as designed prior to transition to the operational phase. In addition, the startup testing program documents the as-built configuration and the initial operating parameters of the facility. The program serves as an opportunity to perform a final system analysis and to detect significant faults prior to facility operation. The startup testing program is also used to confirm the adequacy of training and procedures to be used for facility operation.

The method of testing used in the startup testing program can require analysis, demonstration, examination, inspection, or functional test. The selection of the appropriate test method and scope of the tests are determined using a systematic analysis and are described in ISAR Chapter 3.0, "Conduct of Operations". In general, the startup testing program is a phased program, with successful individual component testing leading to system functional and interface testing, followed by the integrated system testing. A final phase of the program, testing with design waste feed materials, must be successful completed before the facility transitions to an operational phase. Additional information is provided in ISMP Section 3.14, "Commissioning and Operation" and Section 5.6.4, "Commissioning Review".

1.3.15 Operations

The Project safety approach, which began with the design phase and is followed through the construction and testing phases, is also emphasized in the operational phase by establishing a set of principles for achieving excellence in operation of the WTP. This set of principles is implemented as a Conduct of Operations program (see ISAR Section 3.11, "Operational Practices") that controls and conducts the operations of the facility. Attributes of the program include the following.

1) Operation of the facility in accordance with the Technical Safety Requirements
2) The establishment of high standards
3) The communication of those standards to the workforce
4) Provisions for the sufficient number of qualified personnel required to perform the activities necessary to meet the standards
5) Implementation of a philosophy to hold workers and managers accountable for their performance

The conduct of operations program practices are major contributors to the safety of the public and workers. The practices are summarized in the ISAR Chapter 3.0, "Conduct of Operations", and detailed guidance on the practices will be incorporated in the WTP procedures. The conduct of operations program includes shift routines and operational practices (e.g., operator inspection tours, log keeping, response to indications, and resetting protective devices), control area activities (e.g., communications and on-shift training), control of equipment status, lockouts and tagouts, independent verification, operations turnover, required reading, operations procedures, operator aid postings, equipment and piping labels, and incident investigation and reporting.

Another key element in the safety approach is the involvement of operations personnel throughout the design process and the involvement of the design personnel through turnover of the facility to the operations staff (see ISAR Section 3.10.1, "Testing Program Description"). This involvement allows operations personnel not only to provide input to the design process to develop a safe and operable facility, but also to become knowledgeable in the features and limitations of systems and components of the facility. Additionally, the development of facility control system simulators in advance of facility testing strengthens the ability and confidence in the performance of the systems and the operational interfaces. The simulators provide an important integration of the design and operating personnel during the testing in further support of a smooth transition to the operational phase of the project. This interface between the designers, the operators, and the simulators ensures the ability of the Project team to demonstrate operational readiness in advance of final testing activities of the facility.

1.3.16 Configuration Management

Configuration management is one of the fundamental principles to achieve safety. Throughout the life cycle of the RPP-WTP, configuration management is applied to all activities to ensure that programmatic objectives related to radiological, nuclear, and process safety are achieved. Work is performed and controlled to pre-approved plans and procedures that delineate responsibilities. Records that define the requirements, design, verification, and acceptance of the WTP are retained to provide an accurate record of the design including approved changes to the design. Operating organizations define operational requirements and participate in design review, procedure preparation, training, and planning activities to become familiar with the features and limitations of components included in the design of the facility. Organizations that manage or interface with subcontractors or suppliers of items, activities, or services involving configured items flow down applicable requirements to ensure that the configuration management process as defined in the *RPP-WTP Configuration Management Plan* (CM Plan) (BNI 2001f) are properly implemented.

The WTP Configuration Management Program provides direction to identify and document the physical and functional characteristics of facility structure, systems, components, and computer software applications. Its application to design, construction, commissioning, operations, and deactivation activities ensures proposed changes to these characteristics are properly developed, approved, implemented, verified, and incorporated into facility design documentation. The CM Plan is based upon ISO 10007:1995(E), *Quality Management - Guidelines for Configuration Management*.

The project formally identifies and establishes configuration baselines, systematically evaluates and dispositions changes, and records the implementation of approved changes. The Configuration Management Program establishes the policies, guidelines, and responsibilities serving to ensure that:

- The engineered configuration of the project is controlled to ensure it meets design, performance, and acceptance requirements.
- Approved configuration changes are assessed for their impact on performance and safety.
- The configuration status of the technical baseline is maintained.

Configuration management is implemented through project plans and procedures that incorporate requirements from the CM Plan and other top-level requirements documents. Records including Authorization Basis documents; engineering and other source requirements documents; design documents; identification of structures, systems, and components; and links between the design documents and the requirements documents are maintained in an electronic data management system managed by Project Document Control.

Effective implementation of configuration management and supporting processes is assessed through management self-assessments in accordance with approved project procedures. Additionally, formal audits performed by Quality Assurance to their normal auditing practices verify compliance with approved project procedures.

1.3.16.1 Configuration Management Approach

The WTP configuration management program implements a process consisting of four basic steps, as follows:

1) **Identification and documentation.** The activities comprising selection of configured items, documenting their physical and functional characteristics, and allocating unique identification characters and numbers to the configured items and their configuration documents.
2) **Change control.** The activities comprising the control of changes to a configured item after formal issue of its configuration documents.

3) **Status tracking and reporting.** Formal recording and reporting of configuration documents, and the approved changes to those documents.
4) **Configuration audit.** Examination of review, inspection, and test records to determine that a configured item conforms to its configuration documents.

Project plans and procedures fully implement the configuration management process by delineating responsibilities for organizations that manage activities and provide services related to configuration management. Implementing procedures are cited in the CM Plan (BNI 2001f).

1.3.16.2 Configured Item Identification and Documentation

Configured items are selected and documented taking into consideration at what level functional and physical characteristics can be best managed to achieve the overall WTP Project performance objectives related to radiological, nuclear, and process safety. Items identified for configuration management include structures, systems, and components; plant installed software; project interfaces; and Authorization Basis documents.

1.3.16.3 Change Control

Design configuration is controlled in accordance with approved project procedures to maintain an accurate record of the design. Changes are documented to describe the change, the reason for the change, and to identify the configured item and related documents to be changed.

Change control is a formal process comprised of change documentation, evaluation, approval, and implementation.

1.3.16.3.1 Documentation

Changes must be documented except for insignificant changes, i.e., those with no affect on safety, environmental protection, the Authorization Basis, scope, schedule, or cost. When the change control process uses separate change documents, the change documents shall have unique identification numbers for status tracking and convenient to establish links to affected or related documents in the electronic data management system.

1.3.16.3.2 Evaluation

Engineering evaluates proposed changes to identify interface or discipline subject matter impacts and to establish that a proposed change should be implemented. Factors to be considered in the evaluation include compliance of the change with regulations, the Authorization Basis, applicable codes and standards, and safety and environmental significance. Environmental, Safety, and Health monitors the impact evaluation process.

1.3.16.3.3 Approval

The approval process for changes is commensurate, in detail and approval authorities, with the approval process for the original configuration. This may include obtaining authorization from the PSC, customer, or regulators prior to implementing the change.

1.3.16.3.4 Implementation

Approved changes are implemented in accordance with WTP Project procedures identified in the CM Plan specific to the various configured item types encountered in design, procurement, construction, commissioning, operations, and deactivation activities.

1.3.16.4 Status Tracking and Reporting

Status tracking and reporting consists of recording and reporting information required to manage and administer the configuration management process and related activities. Information is recorded, links to related documents entered, and sorted for reporting in the electronic data management system managed by Project Document Control.

1.3.16.5 Configuration Audits

Configuration audit is the examination of items and documents to determine whether a configured items conforms to its configuration documents. Configuration audit typically consists of functional and physical confirmation.

Functional confirmation is accomplished by identifying the individual functional and performance requirements of a configured item and confirming through review, inspection, and test records that the requirements are achieved.

Physical confirmation is accomplished by examining the physical or as-built and tested configured item for compliance to its configuration documents. Together, the functional confirmation and the physical confirmation demonstrate that the configured item, as defined by its configuration documents, conforms to the physical and functional requirements.

1.3.16.6 Functions and Requirements Management

The Contract, *Basis of Design*, *Functional Specification*, *Operational Requirements Document*, and Authorization Basis design requirements are compiled in a~~n Access ©~~ database, designated the Design Criteria Database (DCD). The database has full text and keyword search capabilities. This database is used by design and safety personnel to identify applicable safety functions and requirements for use in the WTP design. The database is updated by procedure each time a source document is revised.

The configuration management organization maintains the *Basis of Design* and DCD to integrate design requirements, safety standards, and operational requirements.

1.3.16.7 Training

The configuration management organization develops, maintains, and provides training on the configuration management program for the project. This training includes a description of the program, reasons why the program is used, the elements of configuration management, and how the program is implemented on the project. This training is provided to employees as part of the Safety and Quality Design Required Training.

1.3.17 Incident Investigations

The importance of the identification and correction of nonconforming conditions as part of a safety approach for the Project is recognized. To ensure that significant incidents that could adversely affect the quality, security, environment, operations, or health and safety of public and workers are brought to the attention of management, the project regulator, and the DOE Occurrence Reporting and Processing System, the ISMP requires incident investigation and reporting. The incident investigations for the Project are expanded in scope to include accidental radionuclide releases and the construction and startup testing phases of the project. Also, reporting of events of less severity than those required of process safety management are included in the program. Incidents to be reported to the regulator include, for example, events or conditions at the facility that resulted in degradation of the principal safety barriers or in a condition beyond the design basis or emergency procedures. The incident investigation process requires that serious events or conditions are addressed and resolved and that the findings of the investigation are resolved.

The investigations are conducted in accordance with the Safety Criteria in SRD Volume II, Section 7.7, "Reporting and Incident Investigation". Additional detail on the implementing procedures are contained in ISAR Section 3.7, "Incident Investigations".

1.3.18 Emergency Planning

An important aspect of the safety approach is to ensure the health and safety of the public and the workers during emergency situations at the WTP. This is accomplished through the development of an emergency management plan for the prompt, efficient, and effective response to emergencies in accordance with the applicable local, state, and federal regulations. The development and the implementation of the emergency management plan are enhanced by the involvement of BNI with the existing Hanford emergency management community. The emergency management plan is fully implemented before radioactive wastes or hazardous chemicals are introduced into the facility. The construction manager implements state and federal emergency preparedness requirements for hazardous situations that may arise during construction.

The scope of the emergency management plan will be determined following the final assessment of the hazards and hazardous situations to be completed during Part B. The implementing procedures will ensure compliance with the applicable requirements that are identified during the development of the emergency management plan. Additional information is included in ISMP Section 3.10, "Emergency Preparedness" and is presented in ISAR Chapter 9.0, "Emergency Management.

1.3.19 Deactivation

All of the previously discussed elements of the WTP safety approach are applied to the deactivation phase of the project.

In addition, the WTP incorporates design provisions to facilitate deactivation and final decommissioning. These provisions reduce radiation exposure to Hanford Site personnel and the public during and following deactivation and decommissioning activities and minimize the quantity of radioactive waste generated during deactivation.

A deactivation plan is prepared prior to construction of the WTP. The deactivation plan provides details on how the following activities will be accomplished to achieve a deactivated status for the facility.

1) Verification of the completion of the facility deactivation end point. (The term facility deactivation end point refers to the set of conditions that comprise the completion of facility deactivation [i.e., radiological, structural, equipment, and documentation])
2) Documentation of the regulatory status, conditions, and inventories of remaining radioactive and hazardous materials and health and safety requirements
3) Modification of the facilities, structures, support systems, and surveillance systems to provide for confinement and monitoring of the remaining contamination, radiation, and other potential hazards
4) Posting and securing of the facility
5) Removal of packaged special nuclear materials and other packaged radiological and chemical materials
6) Confirmation that security systems and procedures are adequate and in place to prevent unauthorized entry