Early Lessons Learned from Risk Applications of DOE Nonreactor Nuclear Facilities

Kevin R. O'Kula
Michael G. Wentink[1]
C. Ray Lux[2]

URS Safety Management Solutions LLC
2131 South Centennial Avenue, Aiken, SC 29803-7680; kevin.okula@wsms.com
[1]Waste Treatment Plant, Bechtel National Inc., Richland, WA, mgwentin@bechtel.com
[2]URS SMS, 2131 South Centennial Avenue, Aiken, SC 29803-7680; ray.lux@wsms.com

Summary

Over the last several years, the Department of Energy (DOE) has taken several actions to provide an infrastructure for providing appropriate controls and support for use of risk assessments and risk informed decisionmaking as it applies to nuclear safety. Three key actions include establishing a Risk Assessment Technical Experts Working Group, revising its Nuclear Safety Policy to explicitly address the use and control of risk assessments, and developing a Draft Standard, "Development and Use of Probabilistic Risk Assessments in Department of Energy Nuclear Safety Applications," (December 2010). The Draft Standard's purpose is "to provide guidance and criteria for a standard approach to utilization of probabilistic risk assessments (PRAs) in nuclear safety applications". In particular, it states, "DOE's nuclear safety decision-making processes can be supplemented and strengthened through application of quantitative and probabilistic risk assessment methodologies; such methodologies may be useful in aiding the evaluation of alternatives that comply with DOE nuclear safety requirements, supporting the USQ process, augmenting traditional safety assessment methods, evaluating changes to DOE safety requirements, and in general, enhancing the quality, transparency, and credibility of analytical results and decisions that are made". Given the publication of the draft standard, significant perspectives can be gained by reviewing past and ongoing efforts where full-scope risk analyses were or are being applied to nonreactor nuclear facilities. In this regard, the objectives of this paper are to review two risk applications performed for DOE nonreactor nuclear facilities, and secondly, to identify the lessons learned from these studies as guidance to the current initiatives on risk-informing safety guidance and design, as well as identifying strengths and limitations of risk assessment to the prospective users, reviewers, and regulators.

The two risk applications selected for this review are for the Defense Waste Processing Facility (DWPF) at the Savannah River, and the Waste Treatment and Immobilization Plant (WTP) at Hanford. The two studies are: (1) the full-scope, Probabilistic Safety Assessment (PSA) for DWPF performed in the 1990s (prior to startup); and the ongoing Quantitative Risk Analysis (QRA) of hydrogen events in WTP.

The key insights identified from these studies are:

- Design and operational vulnerabilities are more easily identified and prioritized on a relative basis than would be from deterministic analysis alone.
- Normal operation tends to contribute appreciably to the total facility risk.
- Much of the value of a PRA approach is from a qualitative, prioritization perspective. The relative risk values are often more useful than the absolute risk values. If the latter are used to inform decision-making then it is critical to be cognizant of the uncertainty or retained margin.
- Although the DOE Draft PRA standard was published relatively recently, it has been useful especially in performance, documentation, risk metrics and peer review areas. In the next issuance of the Standard, it is recommended that a set of simple examples would improve its implementation in the field, either as an appendix or as an implementation guide.
- Applicable reliability data for nonreactor facilities should be carefully considered, especially in the design phase. A recommended path forward is consideration of reestablishing a DOE Complex reliability database that is maintained and updated for support of nuclear nonreactor facility risk applications.

1. INTRODUCTION

U.S. Department of Energy (DOE) directives have long provided a deterministic framework for performing hazards and accident analyses at DOE's nuclear facilities and selecting hazards controls to provide reasonable assurance of adequate public protection. DOE Standard (STD)-3009-94, provides a "safe harbor" in terms of methodology for compliance with Code of Federal Regulations (CFR) Title 10, Part 830, *Nuclear Safety Management,* Subpart B [1, 2]. DOE-STD-3009-94 provides direction on the analyses that are required to support safety basis decisions, and states that the Department's approach does not require or expect the level of detail analysis necessary for a quantitative risk assessment (QRA).

Nonetheless, since initial issuance of DOE-STD-3009 there have been a number of attempts to apply risk application tools. Independent oversight review by the Defense Facilities Safety Board (DNFSB) indicated that DOE contractors had employed risk assessment in a variety of activities, including the development of documented safety analyses and facility level decisionmaking. In time, these observations led to DNFSB Recommendation 2009-1, *Risk Assessment Methodologies at Defense Nuclear Facilities* [3], and the development of a DOE Implementation Plan to resolve the issues and address the concerns articulated in the Recommendation [4]. Part of the Implementation Plan includes evaluation of risk assessment-related polices, standards, guides, and other controls used by other government organizations and industry for applicability to DOE nuclear facilities. Subsequently, DOE has took several actions to provide an infrastructure for providing appropriate controls and support for use of risk assessments and risk informed decision making

as it applies to nuclear safety. These actions included establishing a Risk Assessment Technical Experts Working Group, revising the DOE Nuclear Safety Policy to explicitly address the use and control of risk assessments, and developing a Draft PRA Standard.

Given the publication of the revised DOE Nuclear Safety Policy and the Draft PRA Standard, useful perspectives can be gained by reviewing past and current efforts where full-scope risk analyses were or are being applied to nonreactor nuclear facilities. In this regard, the objectives of this paper are to review past or ongoing risk analyses performed for DOE nonreactor nuclear facilities, and secondly, to identify the lessons learned from these studies as guidance to the current initiatives on risk-informing safety guidance and design, as well as identifying strengths and limitations of risk assessment to the prospective users reviewers, and regulators. In this paper, two specific QRA applications are described to potentially serve as useful prototypes for supplementing deterministic approaches in DOE safety basis applications. Included are: (1) the PSA performed for the Defense Waste Processing Facility (DWPF) at the Savannah River Site (SRS) in the 1990s [5, 6]; and (2) an ongoing QRA for informing design relative to potential hydrogen events at the Hanford Tank Waste Treatment and Immobilization Plant (WTP) [7]. These are compared with the overall approach, methodology and software models to the NUREG-1150 study [8].

2. DOE SAFETY POLICY AND QUANTITATIVE SAFETY OBJECTIVES

This section summarizes two of these actions, i.e., (1) the Draft DOE PRA Standard, and (2) the revised DOE Nuclear Safety Policy.

2.1 Draft DOE PRA Standard

The purpose of DOE Draft Standard, *Development and Use of Probabilistic Risk Assessments in Department of Energy Nuclear Safety Applications*, (December 2010) [9], is "to provide guidance and criteria for a standard approach to utilization of probabilistic risk assessments (PRAs) in nuclear safety applications". In particular, it states, "DOE's nuclear safety decision-making processes can be supplemented and strengthened through application of quantitative and probabilistic risk assessment methodologies; such methodologies may be useful in aiding the evaluation of alternatives that comply with DOE nuclear safety requirements, supporting the USQ process, augmenting traditional safety assessment methods, evaluating changes to DOE safety requirements, and in general, enhancing the quality, transparency, and credibility of analytical results and decisions that are made".

Under its section on applicability and scope, the Draft PRA Standard states it was

- Developed to support use of PRAs in nuclear safety applications.

- Based on standards, guides, and best practices from high-risk industry (chemical, nuclear, and aerospace) on use of risk assessments when used to support risk-informed decision-making in safety applications.
- Also addresses the use of risk assessments to support meeting DOE nuclear safety requirements specified in 10 Code of Federal Regulation (CFR) 830, *Nuclear Safety Management,* related to development and maintenance of documented safety analyses (DSAs) when used to support risk-informed decision-making related to the safety analysis results.

The Draft Standard is directed mostly toward the planning of a PRA application. The planning sections cover key elements in the development of a PRA Plan, including: (1) planning; (2) approach; (3) results, conclusions, and uses; (4) quality assurance and peer review plans. In addition, the performance of the PRA, its documentation, quality assurance and peer review, and peer review results are briefly summarized. Section 5 describes some potential ways that PRAs can be used to supplement DOE's semi-quantitative hazard and accident analysis process to support nuclear safety decisions, including:

- Evaluating Alternative Compliance Approaches
- Supporting the USQ Process (PISA Process)
- Supplementing the Traditional Safety Methods
- Evaluating Changes to DOE Safety Requirements.

The Standard contains an appendix that provides references to offer guidance on how to plan, perform, and apply PRAs to risk-informed decision making in a manner that meets the requirements of this standard. The references provided are drawn from PRA applications at DOE facilities, chemical and process industries, aero-space industry, and the commercial nuclear power industry. An extremely useful set of topical references is included covering:

- Standards for PRA and Risk-Informed Decision Making
- Guidance for Risk-Informed Decision Making
- Non-Reactor PRA Applications
- Guidance for PRA Peer Reviews
- Guidance for PRA Methodology
- PRA Methods for Special Topics.

The PRA Methods for Special Topics section of the table contains a comprehensive set of representative references. Most are nuclear power plant-based but others are listed from other high-hazard industries. Included are references for: Fault Tree Analysis, Database Development and Analysis, Common Cause Failure Analysis, Human Reliability Analysis, Internal Flooding PRA, Internal Fire PRA, External Event Screening, Aircraft Crash Analysis, Seismic PRA, External Flooding PRA, High Winds PRA, Expert Elicitation, Probabilistic Treatment of Phenomena, and Quantification and Treatment of Uncertainties.

2.2 Revision to Nuclear Safety Policy

DOE's Policy (P) 420.1, *Nuclear Safety Policy,* dated 2-08-2011, replaced Secretary of Energy Notice, SEN-35-91, *Nuclear Safety Policy* [10, 11]. DOE P 420.1 includes five high-level "commitments" that define the necessary and sufficient actions that DOE will take to implement its policy (i.e., to assure adequate protection). These actions are briefly summarized as follows:

1. Establish and implement nuclear safety requirements that utilize national consensus (or other government) standards or applicable regulations in accordance with DOE's process for developing and implementing rules, directives and technical standards.
2. Implement core functions and guiding principles of the Integrated Safety Management(ISM).
3. Use a safety management approach that includes minimizing use of hazardous material, and establishing controls that provide defense-in-depth.
4. Allow appropriate use of quantitative and probabilistic risk assessments (PRA) to support nuclear safety decisions.
5. Establish safety goals related to worker and public risk from DOE nuclear facility operations.

These actions are consistent with those defined in the SEN-35-91, but also reflect DOE's adoption of ISM, which incorporated the SEN-35-91 high-level actions for technical competency, safety culture, and roles and responsibilities.

Two quantitative safety objectives (QSOs) are stated at the end of DOE P 420.1 for public protection, and are "aiming points" (not requirements) in support of the Safety Goal that guides the development of DOE's nuclear safety requirements and standards. The two objectives are:

- The risk to an average individual in the vicinity of a DOE nuclear facility for prompt fatalities that might result from accidents 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 population are generally exposed. For evaluation purposes, individuals are assumed to be located within one mile of the site boundary.
- The risk to the population in the area of a DOE nuclear facility for cancer fatalities that might result from operations should not exceed one-tenth of one percent (0.1%) of the sum of all cancer fatality risks resulting from all other causes. For evaluation purposes, individuals are assumed to be located within 10 miles of the site boundary.

The safety goal and associated objectives are adapted from the U.S. Nuclear Regulatory Commission's Safety Goal policy statement for operation of commercial nuclear power plants (51 Federal Register 30028; August 21, 1986) [12]. Quantitatively, the two individual risk objectives[1] are typically evaluated at 5×10^{-7}

[1] Often termed quantitative health objectives (QHOs)

per year and 2 x 10^{-6} per year, for acute fatality risk and latent fatality risk, respectively.

3. EXAMPLE RISK APPLICATION STUDIES

In this paper, two risk application studies are described to provide a basis for lessons learned and insights. The first application of PRA was for the Savannah River Site Defense Waste Processing Facility (DWPF), an operating high-level waste treatment vitrification plant, but was performed in the 1990s prior to the start of operations. The second application is at the Hanford Site and is for the Hanford Tank Waste Treatment and Immobilization Plant (WTP), a larger facility that will perform multiple waste treatment and immobilization functions, but in final design and not yet operational. The WTP application is a Quantitative Risk Analysis (QRA) to risk-inform the design of piping systems, and is currently in progress.

In both cases, the safety analyses associated with these facilities were and are maintained compliant with 10 CFR 830, *Nuclear Safety Management*, Subpart B, Safety Basis, or its identified safe harbor safety analysis methodology contained in DOE-STD-3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis*. The PRAs performed for these facilities, are supplemental analyses performed to evaluate compliance against Safety Goals (in the case of the DWPF application) or establish frequency-severity curves for piping system design relative to postulated hydrogen events (in the case of the WTP application). These studies do not in any way replace or supersede DOE-STD-3009 compliant safety analyses.

However, the special-purpose risk analysis applications prepared for these facilities can provide insights and useful precedents. In particular, these two studies can suggest areas where quantitative risk analysis can supplement deterministic approaches alone. In this manner they can suggest possible starting points for contemporary DOE risk applications.

The next three sections provide review summaries of: (1) the comprehensive Nuclear Power Plant (NPP) PRA study as published in NUREG-1150; (2) the Probabilistic Safety Assessment (PSA) performed for radiological risk evaluation of DWPF for compliance with the DOE SEN 35-91 quantitative safety objective; and (3) the Quantitative Risk Analysis (QRA) performed for risk-informing design of piping systems in WTP.

3.1 NUREG-1150 Summary Overview

The probabilistic risk analysis (PRA) studies underpinning the NUREG-1150 study were based on five plant types. The study was full-scope in that all elements of a Level 3 PRA were performed, was radiological risk focused, and presented several key advances relative to earlier PRA efforts in the 1980s. Some of the more notable improvements included:

- Incorporation of the estimation of the size of the uncertainties in core damage frequency' and risk due to incomplete understanding of the systems

responses, severe accident progression, containment building structural response, and in-plant radioactive material transport;
- Formal elicitation and documentation of expert judgments;
- More detailed definition of plant damage states, improving the efficiency of the interface between the accident frequency and accident progression analyses;
- More detailed definition of plant damage states, improving the efficiency of the interface between the accident frequency and accident progression analyses;
- Types of events and their outcomes explicitly considered in the accident progression and containment loading analyses;
- Analysis of radioactive material releases and the integration of experimental and analytical calculation results into this analysis;
- The use of more efficient methods for estimating the frequency of core damage accidents resulting from external events (e.g., earthquakes); and
- Application of new computer models in the analysis and integration of risk information.

In general, the NUREG-1150 approach to assessment of accident risks could be portrayed with the following characteristics: (1) assesses severe accidents, (2) full-scope, with three levels and (3) design-specific attributes. The NUREG-1150 phases of analysis included: (1) accident frequency, (2) accident progression, (3) containment loading and structural response; (4) transport of radioactive material, (5) offsite consequences; and (6) risk integration analyses. Fault tree and event tree logic models are the main logic methodologies that were applied. Data applied for the reliability of systems, structures and components that are important to safety and to the accident progression are drawn from standardized databases. Some of the major risk analysis software used for NUREG-1150, as well as during subsequent individual plant examinations (IPEs) in the 1990s included: CAFTA (fault tree analysis); EVNTRE (accident progression event tree analysis); Source Term Code Package (source term phenomenological modules), CONTAIN and MELCOR (containment response), LHS (Latin Hypercube Sampling), and MACCS (offsite consequence analysis).

3.2 Probabilistic Safety Analysis for Defense Waste Processing Facility

DWPF is designed to vitrify high-level waste into borosilicate glass forms prior to disposition, and has operated safely for over 15 years. Prior to the start of radioactive waste operations in 1996, a limited scope Probabilistic Safety Analysis (PSA) was performed. The DWPF PSA was a bounding accident analysis with the primary objective of quantifying the maximum credible radiological source terms and the consequences associated with those significant accident types identified from the facility hazard analysis. The PSA included full development of a systems analysis, accident progression analysis, and source term/consequence analysis but did not include full completion of the risk integration and statistical evaluation of phases of the analysis. Following generation of a full range of accident progression

sequences and their associated frequencies, discrete credible sequences were selected for detailed consideration based on consequence estimates and insights gained from completion of a preliminary hazard analysis.

Figure 1 is a schematic of the four primary phases of the DWPF PSA, including a systems analysis, accident progression, bounding accident selection, and source term/consequence analysis. A full set of internal and natural phenomena accident initiating conditions were evaluated, and evaluation of hazards followed the requirements contained in DOE-STD-3009-94, and was a deterministic, systematic consideration of all energy source hazards in the facility, and postulated accident conditions associated with those hazards. From the hazard evaluation, a finite set of potential accident types were identified that characterize and bound the risk associated with operation.

The first major phase was the systems analysis, and followed a classic PRA approach of generating detailed fault trees for each potential accident along with each significant support system. Methodology used to develop accident initiation and support system models, and the data used to quantify the associated occurrence frequencies and conditional failure probabilities followed common nuclear power plant PSA practice. Anticipated releases were estimated outside of the four-phase methodology.

The fault tree models developed as part of the systems analysis phase provided a primary input for the second major phase, Accident Progression analysis. Processing of the support system fault tree models is performed to account for the impact of common support system failures, simultaneous occurrence of events, and interdependency among the individual support systems. The Accident Progression Event Tree (APET) logic model links the initiation of accidents and the failure of support systems with the potential progression of accidents throughout the facility and the performance of facility confinement systems. The accident progression analysis for DWPF was unique in that it also included the modeling of parametric uncertainty in accident progression and system analyses variables, through the statistical sampling of assigned distributions. The output from this part of the analysis consists of a series of potential accident progression sequences and their associated occurrence frequencies. To reduce the large number of sequences, the accident progression analysis output was processed to a manageable number for which detailed quantitative source term and consequence calculations were performed. In the third, or bounding accident selection phase of the risk analysis, offsite consequences were calculated for the resulting subset of processed accident progression sequences. In turn, for each significant accident type identified from the Process Hazards Analysis, a bounding credible scenario was selected to conservatively represent all accident progression sequences of that type.

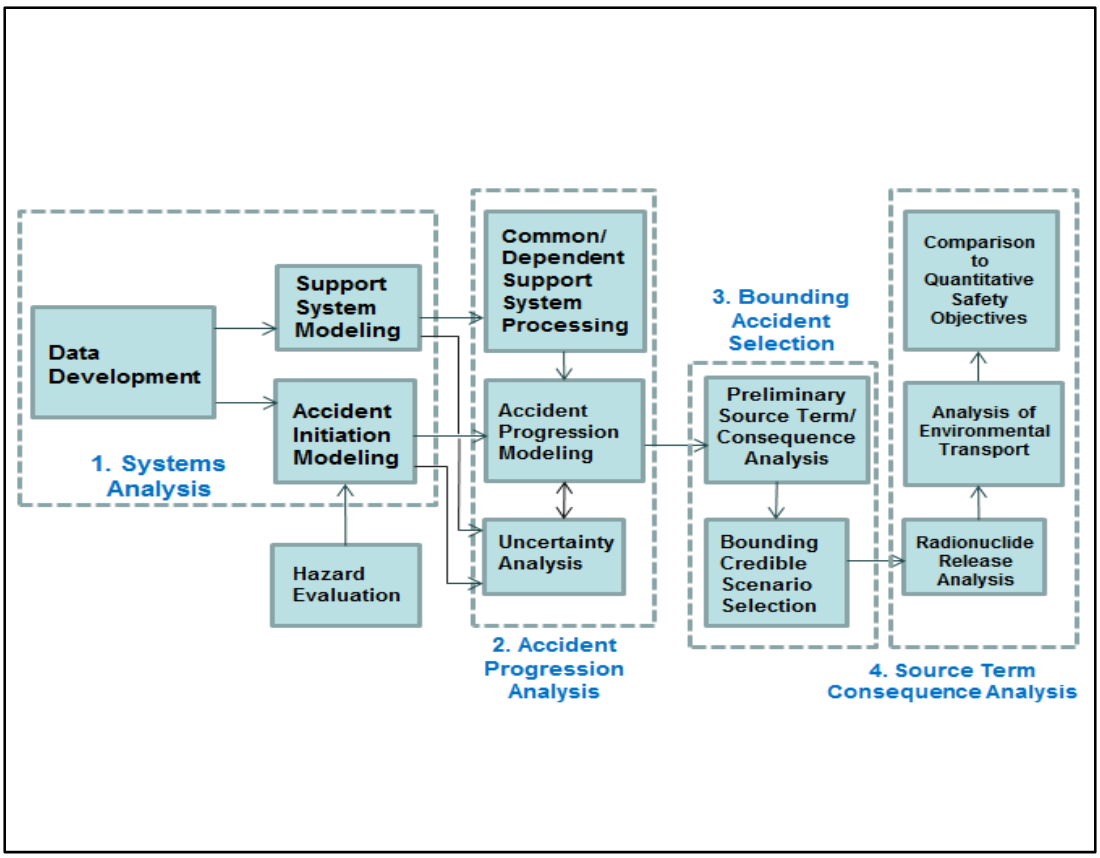

Figure 1. Primary phases of the DWPF Probabilistic Safety Assessment

The final phase of the DWPF PSA was the source term/consequence analysis, in which radiological source terms and consequences were calculated for each bounding credible scenario identified in the preceding phase, and then compared to the QSOs. Doses and individual risks were calculated in two modes. The evaluation mode of interest to the scope of this paper was performed to evaluate DWPF operation relative to the quantitative safety objectives and considered the set of source terms from assumed accident states developed from the APET and the source term algorithm described earlier.[2] Twelve release categories were developed from internal initiating events and twelve were based on external events. Anticipated normal operation conditions were also included. Included in these analyses were general public receptors that may be traveling on thoroughfares through the site and can potentially be exposed at shorter distances than DOE boundary public receptors.

Population doses and interpretation of these doses in the regions of interest relative to SEN 35-91 were calculated [9]. As described earlier, SEN-35-91 was the DOE nuclear safety policy predecessor to DOE P 420.1, containing the same quantitative safety objectives. The average individual prompt fatality risk incurred by the

[2] The other evaluation mode considered the dose for each bounding credible scenario and was compared to the applicable dose criterion. This portion of the analysis is outside the scope of this paper.

population living within one mile of the site boundary was calculated to be identically zero for all 24 internal and external initiating events. The average individual latent fatality risk incurred by the general public living within ten miles of the site boundary was calculated to be 4.5 x 10^{-8} per year, or a factor of more than 40 below the individual latent cancer fatality (LCF) risk safety objective of 2 x 10^{-6} per year. Table 1 shows the total calculated latent cancer risk, and its components.

Table 1. DWPF PSA Latent Cancer Fatality Risk

Source of Risk	Individual Latent Cancer Fatality Risk, (LCF/year)
Normal Operations	4.0E-08
External Events	4.7E-09
Internal Events	4.2E-10
Total	4.5E-08
Safety Goal	2.0E-06

As shown in Table 1, the largest (89%) portion of the calculated individual risk was attributed to normal operations. External events contributed more than an order of magnitude more to individual risk than did internal events.

In summary, the DWPF PSA analyzed environmental releases for both internal and external design basis events, and normal operational conditions. Doses were quantified using the probabilistic approach in the MACCS and MACCS2 software; Short-term (plume passage) effects were considered in the consequence analysis but did not extend to rehabitation (return of the general public to their residence) and food ingestion doses. Equipment and human reliability data were applied based on databases maintained and specific to the DOE Complex. The PSA demonstrated that postulated accidents from the preliminary hazards analysis (PHA) could be analyzed using most of the NUREG-1150 methods (key exception was that accident sequence analysis was not performed) and that both of the quantitative safety objectives were met by wide margins.

Although the DWPF PSA was among the first in the DOE Complex to comprehensively applying reactor based probabilistic methods to quantify SEN 35-91 safety objectives, the PSA was not implemented, or used in any way in the facility's safety basis. However, the use the CAFTA and MACCS/MACCS2 codes has continued to support fault tree and radiological dispersion/consequence work, respectively, in many DOE facilities.

3.1 Quantitative Risk Analysis of Hydrogen Events

WTP is a risk-reduction facility being built to process and stabilize 56 million gallons of radioactive and chemical waste currently stored at the Hanford Site. The Project includes four major nuclear facilities: Pretreatment, Low-Activity Waste Vitrification, High-Level Waste Vitrification and Analytical Laboratory, and will use

vitrification technology to blend high-level waste with glass-forming materials for long-term containment in stainless steel canisters. Construction is expected to be complete in 2016, and the facility operational in the fall of 2019.

The WTP Project is completing a QRA tool to risk-inform the design of individual piping system routes to withstand potential hydrogen combustion loads that may result from deflagration, deflagration-to-detonation transition (DDT), and detonation events associated with the accumulation of hydrogen in its Pretreatment Facility (PTF). The QRA project has been underway since early 2009, and thus predates the December 2010 issuance of the DOE Draft PRA Standard. As noted previously, the QRA is strictly a design tool but can provide information useful to hazard and accident analyses. It is not applied as a surrogate hazards and accident analysis.

While similar in some respects to the nuclear industry PSA in the use of fault tree and event tree logic models, this form of a PRA is more often used in the chemical process industry (e.g., the approach articulated in the Chemical Process Quantitative Risk Analysis (CPQRA) guidance from the Center for Chemical Process Safety (CCPS) [13]). In the case of WTP, the QRA will be applied on a piping system route basis to evaluate potential likelihood and severity of hydrogen events. QRA has long been used in many high hazard industries to prioritize safety, operations, and identify design improvements for systems and facilities based on a spectrum of operational and accident events and their associated frequency-severity conditions. As shown in Figure 2, the QRA is an iterative process will be used to provide the necessary information to analyze piping systems to comply with the allowable strain limits established for WTP piping systems that are subject to potential hydrogen events.

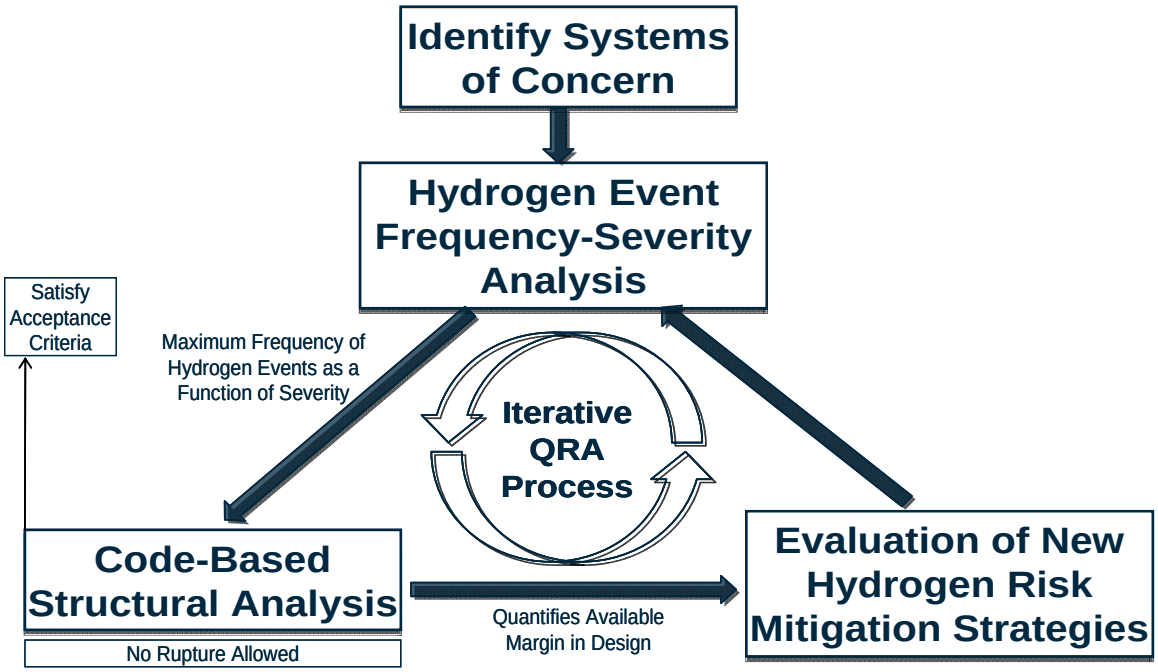

Figure 2. Iterative QRA Process Showing Four Major Task Areas

The QRA consists of the following steps:

1. Identify piping systems that are susceptible to hydrogen accumulation events (e.g., where hydrogen event mitigation controls are not proposed to be used).
2. For each identified piping system, quantify the hydrogen event type, frequency, and severity based on both operational inputs and physical models that describe the progression of a hydrogen event.
3. Quantify the frequency-severity basis that will be used to define the structural evaluation acceptance criteria as defined by ASME[3] for a given route.
4. Perform code-based structural analysis to quantify the available margin in the design using the appropriate acceptance criteria. Implicit in this analysis is that no-breach of the piping system is allowed.

If the structural acceptance criteria are not satisfied, then appropriately modified aspects of the system design, administrative, and/or engineered controls are simulated in the hydrogen event frequency-severity analysis to evaluate potential system modifications.

For each piping system that is analyzed with the QRA, the first step is to quantify the expected frequency and severity of a hydrogen event, and is risk application of interest. The frequency model for this application is termed an Operational Frequency Analysis OFA) logic model, and is based on Version 5.4 of the CAFTA computer code [14]. Both generic and system-specific input parameters are used in a probabilistic model to quantify the frequencies associated with the severities of various types of hydrogen events. Both normal operation and accidental events identified from WTP documentation are used in the frequency analysis to determine the frequency of gas pocket formation in a piping system. Gas pocket formation, duration, and ensuing potential hydrogen events are evaluated in an event tree-based Event Progression Logic model.

The methodology used to determine how the hydrogen event frequency and severity are determined is illustrated in Figure 3. The calculation consists of two stages:

1. Pre-Processing: This is the process where the modeling of the progression of hydrogen events is performed using required inputs including the route configuration inputs, route portioning, operational and frequency analysis (OFA), basic event data, initiating event duration inputs, and physical parameters.

[3] American Society of Mechanical Engineers

2. Monte Carlo Simulation: A Monte Carlo (MC) simulation is used to combine the results of the OFA and event progression logic (EPL) model to determine the frequency and severity of hydrogen events based on both operational

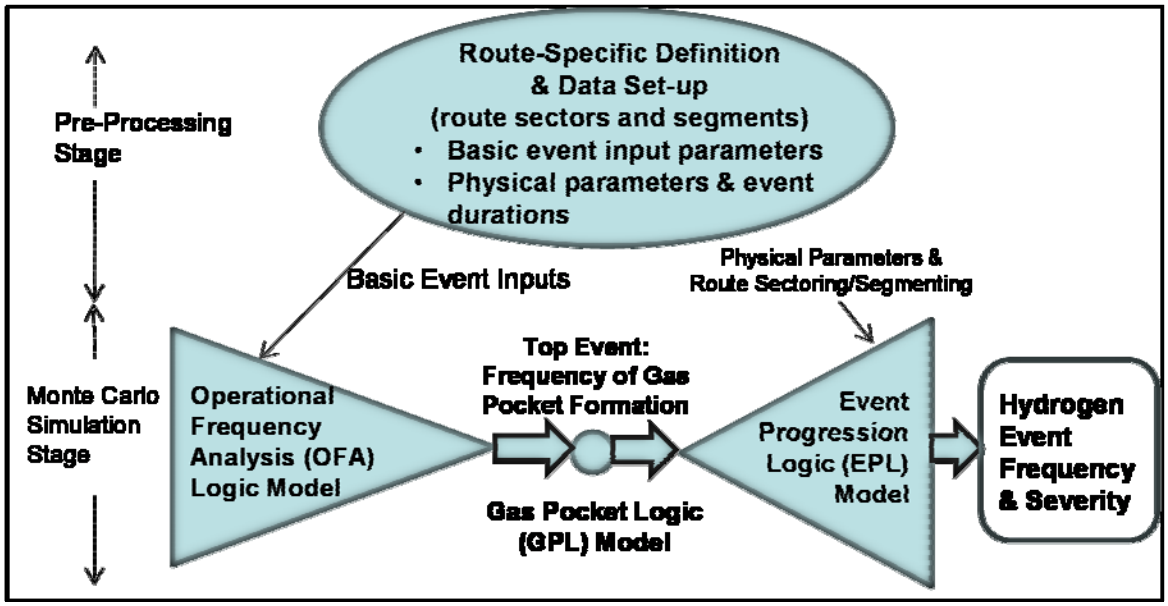

Figure 3. QRA Frequency-Severity Stages and Logic Models

inputs and physical models that describe the progression of a hydrogen event.

The simulation loop contains three main calculation modules:

a. Operation Frequency Analysis (OFA) used to quantify the annual occurrence frequency of gas pockets that can support gas pocket formation.
b. Gas Pocket Logic (GPL) model used to quantify size location and composition of gas pockets in a route
c. Event Progression Logic (EPL) model used to determine the hydrogen event type and quantify the associated severity.

Once the results of all probabilistic trials have been completed, the second step in the QRA process is the quantification of the severity of each hydrogen event type at specific frequency. The resulting hydrogen event types, frequencies, and severities are used to define the appropriate structural loading (i.e., pressure time histories) to be applied to a piping system and analyzed using ASME code-based structural analysis of the code of record to determine if the acceptance criteria are satisfied.

Initiating Events and Input Data

As stated earlier, this paper's focus is limited to the OFA portion of the QRA model. The OFA logic model for a given piping system of interest and its subsequent

minimum cutsets are quantified using Version 5.4 of Computer Aided Fault Tree Analysis (CAFTA). The top event in the OFA logic is gas pocket formation in a portion of the transfer route of interest. Two general types of conditions are modeled as capable of leading to the top event (gas pocket formation, middle of the Figure 3 bowtie): (1) a route-level condition; or, (2) a plant-level condition, that supports gas pocket formation in the subject transfer route portion of the piping. The type of underlying conditions modeled at the route-level are: (1) completed waste transfer with failure to complete hydrogen event mitigation; (2) Unmitigated interrupted waste transfer; and (3) Unmitigated gas accumulation in dead legs (instrumentation or access points in the piping system). Plant-level events include: (1) internal fires; (2) loss of offsite power (LOSP) (non-seismic); (3) seismically-induced LOSP; (4) seismic event; (5) volcanic ashfall; (6) integrated control network failure; and (7) support system failure leads to loss of transfer and hydrogen event mitigation.

Basic event inputs to the QRA include values for equipment failure rates, human error probabilities, failures due to internal and external events (e.g., loss of offsite power), plant-level events, support system events, as well as design information specific to a given route or route portion. Equipment failure rates and human error probabilities are obtained primarily from current nuclear industry and/or DOE applicable standards [15, 16]. External event frequencies were estimated on the basis of from various site and project documents. Route- or portion-specific parameters include BEs that are assigned a value of zero or one to turn on or off specific logic structures or are BEs whose value is dependent on route-specific information. The OFA includes analysis of support systems, including common mode failure analysis implementing the methodology of NUREG/CR-5485 [17].

The QRA of hydrogen events has been reviewed by four independent teams of subject matter experts. Part of this review process included an assessment of the QRA against the requirements and guidance provided in the DOE Draft PRA Standard. One of the reviews commented:

> "The first DOE facility to attempt to use it [the DOE PRA Standard] was the QRA on the Hanford WTP. Although the WTP project could not use the draft standard in the planning stages, the WTP project team performed a detailed evaluation of the QRA against the requirements in the standard and concluded it was able to meet each applicable requirement absent those that would have to be done at the planning stages. The IRT agreed with this conclusion that the applicable requirements had been met. This should be regarded as a success story."

Full implementation of the QRA is anticipated in the near term. However, several preliminary observations may be made regarding the early prototypic use of this tool on selected routes:

(1) Insights have been realized regarding normal operation risk relative to accident initiated risk. Specifically, Routes with dead legs are being reviewed for dead leg placement and location, and whether monitoring/sampling functions could be met otherwise.

(2) Plant-wide conditions present less frequency risk relative to single system upset conditions.

(3) Most of the recovery time distribution risk is from piping route initiated accident conditions.

(4) Single-point failures involving air-operated valves constitute most of the frequency risk. Alternatives are being examined to eliminate these vulnerabilities.

(5) Much of the value of the QRA from an operational risk perspective is as a qualitative, prioritization basis for risk reduction.

Rigorous hydrogen combustion testing was necessary to fill in knowledge gaps and reduce uncertainties, especially in unique areas of hydrogen phenomenology. This phase of the analysis is outside the scope of this paper.

3.2 Top-Level Comparison of NUREG-1150 PRA with the Two DOE Studies

Before collecting overall insights, it is beneficial to compare the NUREG-1150 Light Water Reactor NPP PSA study with those of the risk studies supporting the two DOE facilities. This comparison is provided in Table 2.

In the case of the NUREG-1150 NPPs, the PSAs were performed taking into account postulated severe accident events, plant-specific models, operating data and systems analyses. Industry approaches for equipment reliability were used along with new (at that time) insights into human error (e.g., NUREG/CR-4772 and NUREG/CR-4780) [18, 19]. The nonreactor facility studies focused on design basis accidents identified from the individual facility and site hazards/accident analyses. Normal operation is accounted for in each DOE study that is not considered in the NUREG-1150 analyses.

Each of the NPPs studied in NUREG-1150 had accrued operational experience, ranging from 5 to 18 years. This differs from the DOE studies which were performed on preoperational facilities. The PSA study was completed prior to startup, but after completion of design and operating procedures. The QRA conducted several series of meetings with cognizant and operations staff to model anticipated operating and emergency procedures.

The computer models, applied in the fault tree and Accident Progression Event Tree models for the DWPF study, CAFTA and EVNTRE, respectively, were identical to those applied in the commercial plant NUREG-1150 study. This would be expected considering the narrow time interval (late 1980s to early 1990s) over which the two studies were performed. In the QRA analysis of hydrogen events, CAFTA V5.4 is the software basis for the frequency analysis.

Other characteristics of the Table 2 comparison are explained in the table entry.

Table 2. Comparison of Top-Level Characteristics of Risk Analysis Applications

Characteristic	Risk Study		
	NUREG-1150 PRA Study	**DWPF PSA Study**	**WTP QRA of Hydrogen Events**
Nuclear Facility/Mode	Nuclear Power Plant/ Steady-State, Continuous Operation	Waste Processing, Nuclear, Nonreactor/ Batch Operation	Waste Processing, Nuclear, Nonreactor/ Batch Operation
Facility Design	Standardized PWR and BWR designs; (multiple containment types)	Unique design; confinement system	Unique design; confinement system
PRA type	Radiological Risk; Plant-specific	Radiological Risk; Plant-specific	QRA of hydrogen events; Piping route specific
PRA timing "snapshot" PRA performed & Year of Operation/Start up	Operating plants; Published in 1990: 1. Grand Gulf 1 (BWR-6) - 1985 2. Peach Bottom 2 (BWR-4) – 1974 3. Sequoyah 1 (4-loop PWR) – 1981 4. Surry 1 (3-loop PWR) – 1972 5. Zion 1 (4-loop PWR) - 1973	• Pre-operational • PSA performed in 1993-1994 • Startup in 1996	• Pre-operational • Design of the plant to be complete by 2013 • Construction to be completed in 2016, along with start-up of plant systems • All facilities and systems to be fully operational in 2019
Operational modes	Severe accidents; internal & external initiating events	Design basis events; Normal operation Internal & external initiating events,	Design basis events; Normal operation Internal & external initiating events,
Risk metrics	Acute fatality and latent cancer fatality risks; others; Safety Goal Compliance	Acute fatality and latent cancer fatality risks; others; Safety Goal Compliance	Frequency-Severity curves for different hydrogen event types
Risk output format	Complementary cumulative distribution functions (CCDFs);Safety goal risks @ mean level	Complementary cumulative distribution functions (CCDFs); Safety goal risks @mean level	Complementary cumulative distribution functions (CCDFs); design based on load at the 95th percentile
Fault tree software	CAFTA V1.7 and successor versions	CAFTA, V2.2	CAFTA V5.4
Equipment reliability data	NUREG/CR-2300; NUREG/CR-4550, -4780, others	WSRC-TR-93-262; SRS Fault Tree Data Bank; IEEE 500-1984	NUREG/CR-6928; WSRC-TR-93-262, Rev. 1;
Human reliability data	NUREG/CR-4772	See Table 3 (this paper)	See Table 3 (this paper)
Event tree software	EVNTRE	EVNTRE	Custom-developed, QRA model

3.3 Equipment and Human Reliability Databases

In general, DOE-specific databases were used the frequency analysis in the PRA performed for DWPF. These were both contemporary at the time of the analysis and maintained by the SRS contractor. For the QRA, a peer review recommendation to apply industry data as appropriate was followed. This led to extensive implementation of equipment reliability information from NUREG/CR-6928, while still maintaining use of WSRC-TR-93-262, Rev. 1 [20] in situations where the industry standard was not applicable.

Human reliability data sources were approximately the same in both studies, and followed approximately the same methodology as that performed in the NUREG-1150 study. Table 3 lists the primary sources of reliability and human error data applied in the DWPF studies. Because information on operating procedures for WTP operation is not completed, these have been modeled based on the best available information and discussions with WTP technical staff.

Table 3. Primary QRA Reliability and Human Error Data Sources

Reliability Data Sources
1. WSRC-TR-93-262, Revision 1, "SRS Generic Database Development", and its predecessor.
2. SRS Fault Tree Data Bank
3. IEEE 500-1984, "Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations"
4. Reliability Information Analysis Center (RIAC) Handbook, "Handbook of 217 Plus Reliability Prediction Model"
5. OREDA, "Offshore Reliability Data Handbook"
6. Reliability Analysis Center (RAC, now RIAC), "RAC Automated Data Book"
Human Reliability Data Sources
1. WSRC-TR-93-581, "Savannah River Site, Human Error Data Base Development for Nonreactor Nuclear Facilities (U)", February 1994.
2. NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications", August 1983

4. INSIGHTS FROM NUCLEAR FACILITY RISK APPLICATIONS

The major insights gleaned from the two DOE PRA applications are summarized in this section. Included are those identified from normal operation and postulated accident conditions. In some cases, the insight is gleaned from one study alone; when this is the case, the specific risk application is identified.

4.1 Initial Trial Use of the DOE Risk Standard

While DOE STD-3009 is implemented through a deterministic approach, the DOE PRA Standard acknowledges that "… there are a number of areas where PRA insights can supplement its traditional approaches". Specifically, Section 5.4 of the PRA Standard discusses the areas where PRA approaches can supplement traditional safety methods, noting that "they can also inform the design process, especially for complex, high-hazard facilities".

At the suggestion of one of the QRA peer review groups, the elements of the DOE PRA Standard were compared against the implementation in the QRA, focusing on applicable requirements from Section 4 (Key Elements in Development of PRAs) of the DOE PRA standard. This in effect was a "crosswalk" exercise that compared criterion with an equivalency in the QRA. The net result of this exercise was that the QRA demonstrated general compliance with applicable elements of the DOE PRA Standard.

The December 2010 Draft PRA Standard is weighted towards planning aspects and thus was not a tool applied initially in the planning of the QRA. However, it did guide compliance with important aspects of performance, documentation, quality assurance & peer review. It also alerted the QRA team to additional PRA reference guides and standards from different industries.

4.2 Peer Review Team Composition and Identification of Appropriate Metrics

The DOE PRA Standard also reinforced the QRA's commitment to have adequate and full-scope review, and emphasized the need to identify risk metrics that support the subject the objective of the risk application. The designs of many DOE facilities and their planned operation are often unique, and without a counterpart in the U.S. It is important that peer review teams be assembled to span all technical disciplines required to adequately evaluate the specific risk application in terms of anticipated and/or facility operation, required data for initiating events, equipment reliability and human error probabilities, and phenomenology. Although resource-intensive, these types of reviews in the QRA identified gaps, gave guidance in those technical areas that were deficient, and otherwise improved the overall QRA technical quality.

As indicated earlier, the quantitative safety objective risk metrics from SEN 35-91 (and later DOE's P 420.1, Nuclear Safety Policy) could be applied directly in the case of the PSA analysis. However, the risk metrics applied in the QRA application required several iterations and consideration of the QRA frequency-severity outcome for specific hydrogen events with the deterministic code-based design intent. Ultimately, an independent review team concluded, "A key strength of the QRA developed for the WTP is the innovative use of risk metrics that quantify the

frequency and severity of piping system loads combined with traditional deterministic metrics that can be used with piping design codes, such as ASME B31.3, to provide a high confidence that hydrogen loads will not lead to pipe failures."

4.3 Application of NUREG-1150 and Successor Software Approaches

Methods of fault/event tree logic model development, systems analysis, accident progression event tree application, consequence analysis, and overall risk integration are found as applicable to nuclear nonreactor facilities as they are to NPPs. In particular, models such as CAFTA (PSA and QRA), EVNTRE (PSA), and MACCS2 (PSA), or their contemporary equivalents are found to be readily extended for risk applications in nonreactor facilities.

Specifically, the methodology was flexible and amenable to:

- initiating event and system logic model development and quantification (PSA & QRA),
- integration with an accident progression event tree (PSA) and event progression logic (QRA) models, and
- quantification of dose, health effect and quantitative safety objectives with MACCS/MACCS2 (PSA).

4.4 Compliance with Quantitative Safety Objectives

The PSA performed for radiological releases in DWPF provided insights in acute latent quantitative safety objectives for nonreactor nuclear facilities.

4.4.1 Acute Fatality Risk

The DWPF PSA study showed identically zero acute fatality risk due to postulated accident conditions at any level of consequence within a mile of the DOE reservation boundary.[4] In addition, MACCS2-calculated acute risk posed by the facility to collocated workers was also found to be identically zero. This is due to primarily two factors: the source term and secondly, the distance to receptors. Nonreactor nuclear facilities have insufficient source term both in magnitude and type of radionuclides released. A NPP source term has appreciable quantities of short-lived, noble gases and radioiodine in its inventory, with external radiation potential. In contrast, for all but inadvertent criticality source terms, nonreactor facilities are characterized by relatively longer-lived, alpha-emitting radionuclides that are primarily inhalation hazards [NUREG-1140]. In general, *credible* criticality events in most nonreactor nuclear facilities will not be large enough to cause acute risk effects outside the facility, given most distances to the facility and site boundaries.

[4] The analysis also included members of the general public traveling on thoroughfares through the DOE site.

Thus, in nonreactor, nuclear waste processing facilities, coupled with most site boundary distances, sufficiently large enough source terms occurring relatively early in the accident sequences, and containing radionuclides potentially leading to acute health effects are simply not credible.

4.4.2 Latent Fatality Risk

The latent risk determined in the earlier PSA analysis is more than a factor of 40 lower for DWPF than the quantitative safety objective of 2.0×10^{-6} per year. This is due to type of source term present in these fatalities, coupled with the recognition that even the largest source terms do not have sufficient inventory, and requisite airborne release fractions to pose a challenge to the average individual in the 10-mile region from the DOE boundary. Specifically, the PSA demonstrated that the mean LCF risk to the onsite workers in the ten-mile region from the facility boundary was 2.4E-07 LCF/year for DWPF, or approximately an order-of-magnitude below the public quantitative safety objective.

4.5 Relative Importance of Normal Operations and Accident Conditions

Use of risk application methods provided information on the relative contributions of normal operations and postulated accident conditions. Consideration of normal operation provides two distinctly different perspectives on overall operation of nonreactor facilities. In the case of the DWPF analysis, the PSA for radiological LCF risk for DWPF is chiefly due to routine, anticipated releases. Faulted (accident) conditions while having larger source terms are weighed by much less likely occurrence frequencies, and constitute about approximately 20% of the latent risk.

In the WTP QRA piping routes with non-flow sections of piping (dead legs), the importance of these locations to operational risk was identified through the QRA. These QRA-informed indications provided a checkpoint to see if there are obvious changes that can be made in design for instrumentation and sampling, or if modeling assumptions and use of data are being applied correctly.

4.6 Identification of Appropriate Component Data

The identification of reliability data available in 1990s PSA application was based on applicable, generic databases maintained at many sites for general use throughout the DOE Complex. In the case of current risk applications, many basic event data are found directly from the commercial industry sources such as NUREG/CR-6928 and IEEE 493 sources. However, these sources are not always directly transferable due to the type of equipment and the anticipated operating environments.

Periodic review of the relevant databases and their applicability to the facility of interest will be needed as some of the older DOE data collections are no longer being maintained. This is especially important for facilities where a mix of nuclear and chemical facility data are required.

5. CONCLUSIONS AND RECOMMENDATIONS

A summary review has been completed of an early-1990s Probabilistic Safety Assessment (PSA) of a nonreactor, nuclear waste processing facility, and an ongoing Quantitative Risk Analysis (QRA) of a newer waste processing facility with respect to nuclear power plant (NPP) risk applications. The PSA was performed using methodology similar to those used in PSAs evaluated as part of the 1990 NPP plant NUREG-1150 study, and focused on radiological risk. The QRA is still ongoing, and is being applied to inform the design of piping systems relative to potential hydrogen events. The review was performed to identify insights from the early work and to guide those planning new risk studies in the DOE/NNSA Complex.

Neither the PSA nor the QRA are part of the respective facility's safety basis. Both studies were of pre-operational facilities using the best available information on design, planned operation, and hazard and accident analysis documents.

The main conclusions of this review are as follows:

- Design and operational vulnerabilities are more easily identified and prioritized on a relative basis than would be from deterministic analysis alone.
- Normal operation tends to contribute appreciably to the total facility risk.
- Much of the value of a PRA approach is from a qualitative, prioritization perspective. The relative risk values are often more useful than the absolute risk values. If the latter are used to inform decision-making then it is critical to be cognizant of the uncertainty or retained margin
- While issued only recently, the DOE Draft PRA Standard (December 2010) was useful in later stages of the QRA. Principally, it guided compliance with important aspects of performance, documentation, quality assurance & peer review. It also alerted the QRA to additional PRA reference guides and standards from different industries.
- The DOE PRA Standard has been particularly beneficial in recognizing the need of a robust peer review process and identifying and applying risk metrics particularly in risk applications that depart from traditional radiological risk applications.
- The early 1990s DWPF PSA analysis, a radiological risk application, illustrated the extension of many of the NPP PRA tools and methods to nonreactor nuclear facilities. The PSA demonstrated that postulated accidents from the preliminary hazards analysis (PHA) could be analyzed using most of the NUREG-1150 methods (key exception was that accident sequence analysis was not performed) and that both of the quantitative safety objectives were met by wide margins.
- Preliminary observations from the WTP QRA, a non-radiological risk application, regarding the early prototypic use of this tool on selected piping routes includes:
    - Insights have been realized regarding normal operation risk relative to accident initiated risk. Specifically, Routes with dead legs are being

reviewed for dead leg placement and location, and whether monitoring/sampling functions could be met otherwise.

- Plant-wide conditions present less likelihood relative to single system upset conditions.
- Most of the recovery time risk is from piping route-specific initiating events (postulated equipment failure, human error, etc.).
- Single-point failures involving air-operated valves constitute most of the equipment frequency risk. Alternatives are being examined to eliminate these vulnerabilities.

Two recommendations were developed through this review, one on examples of successful risk applications and a second on updating reliability data. In the next issuance of the Standard, it is recommended that a set of simple examples would improve its implementation in the field, either as an appendix or as an implementation guide. One possible model would be the DOE-STD-5506 TRU Waste Standard.

Another outcome of this review is that while most equipment reliability data can be obtained from nuclear industry sources, such as NUREG/CR-6928, this database and others may not always be the best and most applicable data for component reliability data and initiating event frequency. DOE sites and lead facilities previously maintained fault tree and event tree logic model data through much of the 1990s (e.g., SRS Fault Tree database). But the usefulness of these data collections if still accessible may not be as relevant to today's high-hazard facilities due to data quality and maintenance issues. A suggested improvement to this situation is development of an updated database for nuclear nonreactor facilities, including use of international sources. This improvement could be sponsored under the Safety Analysis Working Group of the Department of Energy Facility Contractors Group (EFCOG).

6. ACKNOWLEDGMENTS

The authors acknowledge the significant roles of Ryan Jones and Jean Collin of Dominion Engineering Inc., Carl Benhardt of URS SMS, and Sarah Lachmann of BNI in the development and implementation of the QRA model. We also appreciate the early efforts of many colleagues including Jackie East (and many others too numerous to credit individually) that were part of the SRS PSA project in the early 1990s.

7. REFERENCES

1. U.S. Department of Energy, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, DOE-STD-3009-94, Change Notice 3. Washington, D.C., March 2006.
2. 10 CFR Part 830, Nuclear Safety Management, Subpart B, Safety Basis.
3. Defense Nuclear Facilities Safety Board, *Risk Assessment Methodologies at Defense Nuclear Facilities,* Recommendation 2009-1, Washington, D.C. (July 30, 2009).
4. U.S. Department of Energy, *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2009-1*, *Risk Assessment Methodologies at Defense Nuclear Facilities*, DNFSB Rec. IP Rev. 1, March 2010, Washington, D.C., March 2010.
5. Westinghouse Savannah River Company, DWPF Mode C Probabilistic Safety Analysis (U), WSRC-TR-95-0198, Aiken, South Carolina, (June 1995).
6. East, J.M. and K.R. O'Kula, *A Comparative Study of Worker and General Public Risks from Nuclear Facility Operation using MACCS2(U)*, WSRC-MS-94-0406, International Conference on Mathematics and Computations, Reactor Physics, and Environmental Analyses, Portland, Oregon, (April 26 – May 1, 1995).
7. Bechtel National, Inc., *Quantitative Risk Analysis of hydrogen events at WTP: Development of Event Frequency-Severity Analysis Model*, 24590-WTP-RPT-ENG-10-008, Rev. 3, Richland, WA, (2011).
8. U.S. Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, Washington, D.C. (Dec. 1990).
9. U.S. Department of Energy, *Development and Use of Probabilistic Risk Assessments in Department of Energy Nuclear Safety Applications*, Draft DOE Standard, DOE STD-xxxx-xx, (December 2010).
10. U.S. Department of Energy, *Department of Energy Nuclear Safety Policy*, DOE P 420.1, Washington, D.C. (Approved 02-08-2011).
11. U.S. Department of Energy, *Nuclear Safety Policy*, Secretary of Energy Notice SEN-35-91 (September 1991).
12. 51 Federal Register 30038, Safety Goals for the Operations of Nuclear Power Plants. Originally published 8/4/86 and republished 8/21/86 with corrections.
13. Center for Chemical Process Safety, Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition, American Institute of Chemical Engineers, New York, NY. 2000.
14. Electric Power Research Institute, Inc. (EPRI), *CAFTA, Fault Tree Analysis System, Version 5.4,Software Manual*, ID #1018460, CD-ROM, Palo Alto, CA, 2009.
15. NUREG/CR-6928, *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*, Idaho National Laboratory, Idaho Falls, ID, February 2007.
16. Westinghouse Savannah River Company, *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)*, WSRC-TR-93-581, February 1994.
17. U.S. Nuclear Regulatory Commission, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, November 20, 1998.

18. U.S. Nuclear Regulatory Commission, *Accident Sequence Evaluation Program-Human Reliability Analysis Procedure*, Sandia National Laboratories, NUREG/CR-4772, SAND86-1996, February 1987.
19. A. Mosleh et al., *Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Procedural Framework and Examples*, NUREG/CR-4780, Vol. 1, EPRI NP-5613, January 1988.
20. Westinghouse Savannah River Company, *Savannah River Site Generic Data Base* (WSRC-TR-93-262, Rev. 1, May 1998.