NUCLEAR ENERGY RESEARCH INITIATIVE

Risk Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants
(Cooperative Agreement DE-FC03-99SF21902, Am. M004)

Final Technical Report

Report # DOE/SF21902
(Internal: #RISK-G-001-2003)

January 29, 2003

Prepared for the United States Department of Energy,
Office of Nuclear Energy, Science, and Technology

Issued by Westinghouse Electric Company

Table of Contents

Executive Summary

This document provides the final technical summary report to the Department of Energy (DOE) for this just-completed project. In previous project years, final reports on four of eleven subtasks were issued. This year, work on the remaining seven subtasks has been completed and corresponding reports have been issued. This final technical report summarizes the specific activities accomplished, provides an overview of results achieved, and indicates how the results can be implemented for an actual new design project.

Background and Goal: The DOE established the Nuclear Energy Research Initiative (NERI) to address the barriers to long term use of nuclear-generated electricity in the United States. In addition, the Electric Power Research Institute has continued to perform studies on the cost of coal, gas, and nuclear-generated electricity. To be competitive, the cost for the nuclear option would have to decrease to the range of 3 cents/kilowatt-hour over the next two decades. Correspondingly, the total plant capital cost would have to decrease by about 35% to 40% relative to large evolutionary Advanced LWR cost estimates, and the construction schedule would have to be shortened to about three years in order to ensure nuclear-generated electricity would be economically competitive.

In response to the above developments, Westinghouse Electric Company (formerly ABB Combustion Engineering Nuclear Power) initiated a cooperative effort with Sandia National Laboratories and Duke Engineering & Services on an innovative research program proposal with the goal of meeting the above cost reduction targets for new nuclear power plant construction. The vision for this cooperative effort is to meet the cost-reduction goals through implementation of new technology and innovative approaches to the design and licensing of new nuclear power plants. DOE approved three separate projects that have similar overall objectives of reducing nuclear power plant costs. These three projects are "Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants" led by Westinghouse, "Smart Nuclear Power Plant Program" led by Sandia National Laboratories, and "Design, Procure, Construct, Install and Test Program" led by Duke Engineering & Services. The duration of the Risk-Informed Assessment project is approximately 2.6 years and DOE is expected to provide funding of $2.5 million. Westinghouse partners in this project are Egan & Associates, Duke Engineering & Services (now Framatome/ANP), Massachusetts Institute of Technology, North Carolina State University, Sandia National Laboratories, and Idaho National Engineering & Environmental Laboratory.

Approach and Benefits: The Risk Informed Assessment of Regulatory Requirements project includes two basic tasks: (1) "Development of Risk-Informed Methodologies" and (2) "Strengthening the Reliability Database." The primary benefit of this project is the development of methods for a new, highly risk-informed design and regulatory process. For the first task, specific subtasks are: (1) identify all applicable current regulatory requirements and industry standards; (2) identify systems, structures, and components (SSCs) and their associated costs for a typical plant; (3) develop a methodology for risk-informing the requirements and standards; (4) develop a methodology for risk-informing the design of SSCs; (5) identify those requirements, standards, and SSCs that should be given the highest priority; (6) demonstrate the methodologies by applying them to a sample SSC; (7) evaluate the current regulatory processes at the Nuclear

Regulatory Commission (NRC); and (8) coordinate these activities with the currently ongoing efforts of the Nuclear Energy Institute (NEI), NRC, and industry.

The second basic task is the strengthening of the reliability database that will be needed to evaluate the safety and reliability of future nuclear power plant designs. Plant designers will need to demonstrate that their new plant designs satisfy NRC safety goals. This will require good, defensible reliability data for equipment. Specific subtasks for this effort are: (1) identify current sources of reliability data, (2) identify weaknesses in data sources, and (3) develop proposed programs for correcting the weaknesses.

Issues and Accomplishments: Shortly after initiating Phase 1 of this project, team members agreed that a very basic change to the current method of design and regulation was needed. It is believed that the cost reduction goal could not be met by making relatively minor adjustments to the current system (i.e., an evolutionary approach). Rather, it is believed that a new, more advanced, approach is needed and that a completely new design and regulatory process would have to be developed – a "clean sheet of paper" approach. This new approach would (1) start with risk-based probabilistic methods, (2) establish probabilistic design criteria, (3) model - to the extent practical - all design and regulatory issues in probabilistic terms (vs. deterministic terms), and (4) implement deterministic judgements only when necessary to meet basic, over-arching safety issues (e.g., allocation of risk between prevention and mitigation functions). Design and regulatory issues (e.g., equipment performance uncertainties, safety margin, etc.) would be modeled probabilistically so that they can be evaluated in the context of overall plant performance and safety. This new approach is different from the current risk-informed design and regulatory process used by industry and the NRC because the evaluation of uncertainties and safety margin is done in the context of an integrated probabilistic model, not through independent and sometimes arbitrary judgements.

The work performed in Phases 1–3 of this project has produced (1) a generic methodology for a new risk-based design and regulatory process, (2) an example of applying the new process to the design of light water reactors along with supporting thermal-hydraulic analyses and probabilistic risk assessments, (3) an example of a desired regulatory interaction using the new process, and (4) an application of the new process to a sample problem for a gas reactor to show the applicability of the new process to designs other than light water reactors. Future development of this new methodology should include new methods for addressing uncertainties in Probabilistic Risk Assessments, including probabilistic treatments of material properties in the design of structures and components, and strengthening the supporting reliability database.

Deliverable, Schedule, and Cost Summary: Reports and documentation for all three phases of this project were produced generally on schedule. This Final Technical Report summarizes all significant results and references specific subtask reports for more detailed descriptions.

Cost summary reports are provided herein. Month-by-month actual costs were not always as planned, but total actual costs at the end of each project year were close to plan, due in part to modest extensions of the project year ending dates (requested by Westinghouse and approved by the DOE).

1.0 Introduction

1.1 Background

The major impediment to long term competitiveness of new nuclear plants in the U.S. is the capital cost component -- which will need to be reduced on the order of 35% to 40% for Advanced Light Water Reactors (ALWRs) such as System 80+ and Advanced Boiling Water Reactor (ABWR). The required cost reduction for a passive ALWR such as AP1000 would be less. Such reductions in capital cost will require a fundamental re-evaluation of the industry standards and regulatory bases under which nuclear plants are designed and licensed.

The current collection of nuclear industry standards and NRC regulatory requirements includes primarily deterministic criteria, based largely on qualitative risk assessments and engineering judgment that evolved over the last forty years of the nuclear energy industry. Many of the current industry standards and regulatory criteria are not significantly contributing to reliability and safety and, therefore, have needlessly driven the costs of new nuclear plants into a range that is not economically competitive in the U.S. market.

The state-of-the art for probabilistic risk assessment (PRA), including the database of operating experience, is now sufficiently mature that we should be able to develop a new, highly risk-informed design and regulatory process that maintains high levels of reliability and safety while decreasing plant capital and construction costs. Although humans must always make the final decisions, the decision process should now be able to rely much more heavily on risk-informed inputs. The Nuclear Energy Institute, the NRC, and the rest of the nuclear industry are already working together to apply risk-informed, performance-based regulation to the licensing of existing plants. Though still in the early stages, this industry/NRC effort is making progress and promises to offer substantial benefits. However, these efforts are focused only upon the requirements that affect operation and maintenance of existing nuclear plants.

What is needed, beyond the current effort, is to apply a more aggressive risk-informed approach to those issues that affect the design and licensing of new plants, rather than just the operation and maintenance of existing ones. This project is developing the methodologies needed for such an aggressive program. Since this research effort is coordinated with the ongoing industry/NRC effort for existing plants, it is intended to complement that ongoing program, rather than duplicate it or compete against it.

In addition, a new approach is needed for new plant designs (e.g., gas-cooled pebble bed reactors) that are significantly different from today's ALWRs to avoid unnecessary design margins based sometimes-arbitrary judgements. Rather, current plant experience would be evaluated along with new design features and technology in the context of an integrated probabilistic risk assessment. Fortunately, there is now an increasing awareness that many of the existing regulatory requirements and industry standards are not significantly contributing to safety and reliability and, therefore, are unnecessarily adding to nuclear plant costs. Not only does this degrade the economic competitiveness of nuclear energy, it results in unnecessary costs to the American electricity consumer. This research project has been coordinated with current efforts of industry and NRC to develop risk-informed, performance-based regulations that affect the operation of the existing nuclear plants and has gone further by focusing on the design and regulatory process for new plants.

1.2 Vision

The overall goal of this research project was to support innovation in new nuclear power plant designs. This project examined the implications, for future reactors and future safety regulation, of utilizing a new risk-informed regulatory system as a replacement for the current system. This innovation was be made possible through development of a scientific, highly risk-informed approach for the design and regulation of nuclear power plants. When fully implemented, this approach would include the development and/or confirmation of corresponding regulatory requirements and industry standards.

To understand the need for a new, highly risk-informed design and regulatory process, it is worthwhile to first step back and look at an example of how the current design and regulatory requirements and standards evolved – and why they may no longer be appropriate. For such an example, let's look at the design of the Safety Injection System (SIS) and its design basis event, the loss of coolant accident. Beginning over thirty years ago, a great number of deterministic regulatory criteria have been developed for the SIS, based upon a postulated event that is now known to have a negligible chance of occurrence: an instantaneous double-ended guillotine pipe break, in the worst location, with the worst single failure, with the worst initial conditions, with the worst operator response, with the worst coolant-radioactivity conditions, with the worst containment leakage, etc., etc. Industry standards and NRC regulatory requirements for the SIS evolved in a patchwork of documents that were generated or revised every time someone thought of a new concern, there was a new problem at an operating plant, or something was found during maintenance. These requirements are found in a number of documents that include the Code of Federal Regulations, regulatory guides, standard review plans, IE bulletins, etc. In many cases, industry standards (e.g., portions of the ASME Code) were developed and referenced in the NRC documents. Because many of these requirements were put in place many years ago, they were not subject to cost/benefit evaluation. Even if they had, they would have been evaluated separately, one by one. There has never been a complete assessment of how all of the requirements – taken together as a package – would be evaluated in a comprehensive cost/benefit analysis.

After the first PRAs were performed in the 1970s (e.g., WASH-1400), it was recognized that the most catastrophic events imaginable were not the events most likely to threaten public safety. The double-ended guillotine pipe break was found to be of such low probability that, by the early 1980s, the NRC's Materials Branch acknowledged that ductile pipe would "leak before break" and, therefore, could not pose a real threat -- as long as there was a leakage detection system. On this basis, the NRC allowed "leak before break" to be credited, in satisfying some of the *new* requirements that NRC was then imposing (e.g., for asymmetric blowdown loads). However, the double-ended guillotine pipe break was still maintained as the basis for the already established NRC requirements -- which had served as the design basis for almost everything in the nuclear island (e.g., the SIS, containment, etc.). This obvious inconsistency in regulatory requirements was accepted by NRC and industry as providing an added safety margin to cover the unknown.

In a young industry - lacking a wealth of operating experience and data - added safety margin, to cover the unknown, was not unreasonable. Furthermore, in a regulated electricity industry, the added requirements could be tolerated because plant owners could usually pass along the costs of satisfying the NRC requirements to ratepayers. However, in the coming deregulated power market, continuing the use of design features that do not truly add to safety and reliability will result in nuclear plant designs that are not cost competitive against other electricity generating options - and, therefore, will simply not be purchased.

Implementation of a new "highly risk-informed" design and regulatory process in actual reactor design projects would enable a more efficient, science-based regulatory process and improved plant designs. The methods developed in this project represent an advance in the science of risk management. Further, implementation of the new methods would provide the capability to rapidly evaluate plant design changes, which will facilitate innovation for new plant designs and streamline the regulatory review process.

1.3 Summary of Results and Potential Implementation Benefits

In the first year of this project, a framework for a more highly risk-informed design and regulation process was drafted based primarily on the Light Water Reactor experience base. Due to (1) the accrual of significant design and operating experience over the past several decades, (2) the development of improved PRA capability and experience within both the industry and the Nuclear Regulatory Commission, and (3) the observation that efforts to risk-inform a few of the regulations for and design features of currently operating plants was a very slow and complex process, it was decided by this project's team to not follow the "evolutionary" path being followed for currently operating plants. Rather, it was decided to start with a "clean sheet of paper" in order to develop new methods based on operating experience, equipment performance databases, and current analytical technology, but not to be burdened by past assumptions and judgments on design margin and "defense-in-depth" that are not justified by logical, technical analysis. The new approach would include all the elements of the current design and regulatory process, however, the PRA would be used as the primary decision making tool and design margin and defense-in-depth would be used only when the specific uncertainties could not be satisfactorily addressed in the PRA.

A sample design change for the System 80+ ALWR was evaluated using the newly proposed methods. It was demonstrated that, based on more recent data for pipe break probabilities, the large pipe double-ended LOCA and single failure criteria could be eliminated from the plant design basis without a significant reduction in the predicted Core Damage Frequency. As a result, this example showed that it could be possible to eliminate a significant amount of equipment from safety systems and even combine some safety and normal operation functions – a notable departure from current design and regulatory thinking. Another first-year activity addressed the investigation of risk-informed methods for design of structures and piping systems. Sample analyses showed that in some cases, loads on piping systems and supports, due in part to structural interactions, could be reduced by approximately a factor of ten. Other first-year work included interfacing with industry (Nuclear Energy Institute) and the NRC and a comprehensive review of existing databases that support nuclear plant design and operation.

In the second year of this project, the framework was refined and the sample analyses were extended to include the System 80+ normal and emergency feedwater systems – with similar results. KOPEC was added as a collaborator and they worked on thermal-hydraulic analyses to support the PRA. An example of an NRC design review using the new risk-based methods was developed and a report was issued that summarized improvements to the licensing process defined in NRC's regulations. This project interacted with the industry, including interfacing with an ASME code development task force on risk-informing ASME design codes. In addition, reports were issued to summarize (1) the sources of NRC and industry criteria for design and regulation of nuclear power plants, (2) costs associated with plant design components and risk-informed design improvements, and (3) database usage weaknesses and software to facilitate their use.

In the third year of this project, the new design and regulatory framework was refined to ensure its applicability to non-LWR technology, using a pebble-bed gas reactor as an example. Accordingly, a PRA analysis was performed for the gas reactor example to show the process for evaluating specific design features. The analysis showed that an LWR-containment might not be required. That is, the containment function could be accomplished with a "confinement" building (much less costly) while still meeting safety criteria. KOPEC performed additional PRA and thermal hydraulic analyses and work on risk-informing the ASME piping design codes was refined. Finally, reliability database issues were summarized and improvement approaches were outlined.

2.0 Project Goals and Organization

2.1 Goals

The overall goal of this research project is to support innovation in new nuclear power plant designs. This project is examining the implications, for future reactors and future safety regulation, of utilizing a new risk-informed regulatory system as a replacement for the current system. This innovation will be made possible through development of a scientific, highly risk-informed approach for the design and regulation of nuclear power plants. When fully implemented, this approach would include the development and/or confirmation of corresponding regulatory requirements and industry standards. The major impediment to long term competitiveness of new nuclear plants in the U.S. is the capital cost component -- which may need to be reduced on the order of 35% to 40% for Advanced Light Water Reactors (ALWRs) such as System 80+ and Advanced Boiling Water Reactor (ABWR). The required cost reduction for a passive ALWR such as AP1000 would be less. Such reductions in capital cost will require a fundamental re-evaluation of the industry standards and regulatory bases under which nuclear plants are designed and licensed. In addition, a new approach is needed for new plant designs that are significantly different from today's ALWRs to avoid unnecessary design margins based sometimes-arbitrary judgements. Rather, current plant experience would be evaluated along with new design features and technology in the context of an integrated probabilistic risk assessment. Fortunately, there is now an increasing awareness that many of the existing regulatory requirements and industry standards are not significantly contributing to safety and reliability and, therefore, are unnecessarily adding to nuclear plant costs. Not only does this degrade the economic competitiveness of nuclear energy, it results in unnecessary costs to the American electricity consumer. This research project has been coordinated with current efforts of industry and NRC to develop risk-informed, performance-based regulations that affect the operation of the existing nuclear plants and has gone further by focusing on the design and regulatory process for new plants.

The above goal is being achieved through the following two major tasks (objectives):

?? **Task 1: Development of Risk-Informed Methodologies:** Many of the regulatory requirements and industry standards that form the bases for designing the current generation of nuclear plant designs are based upon subjective, deterministic assumptions that were limited by the knowledge-base and engineering tools that were available at the time that those requirements and standards were created. The research effort proposed for this project is to develop a set of risk-informed methodologies that can be used by future plant designers to (1) systematically develop and/or utilize all of the regulatory requirements and industry standards that would impact the design of new nuclear plants and (2) systematically develop designs for a nuclear plant's SSC's, by applying those methodologies. This research effort will be complementary to the current industry/NRC efforts to apply risk-informed, performance-based regulation to selected issues that affect operation of existing nuclear plants. The methodologies developed in this research project will then be demonstrated, by applying them to a sample problem. The methodologies may then be revised to apply the lessons learned from this sample.

?? **Task 2: Strengthen the Reliability Database:** To fully risk-inform the design bases for future nuclear plants, it is essential that the reliability database for the SSC's be complete. Current industry/NRC efforts to strengthen the reliability database are primarily focused upon issues that affect operation of the existing nuclear plants. The research effort proposed for this project will identify where strengthening of the risk assessment database is needed to support the design of new plants – including identification of the reliability information that will be needed to support introduction of new, advanced “smart” technologies. The research effort will also recommend programs for collecting the information that will be needed by future plant designers, to provide this information.

2.2 Organization

Work for this project is organized according to the following work breakdown structure:

2.2.1 Task 1: Development of Risk-Informed Methodologies

?? Subtask 1.1: Identify applicable current regulatory requirements and industry standards.
?? Subtask 1.2: Identify systems, structures, and components (SSCs) and their associated costs for a typical plant.
?? Subtask 1.3: Develop methodology for developing risk-informed requirements and standards.
?? Subtask 1.4: Develop methodology for designing highly risk-informed SSCs.
?? Subtask 1.5: Identify high priority requirements, standards, and SSCs.
?? Subtask 1.6: Apply methodologies to a sample SSC.
?? Subtask 1.7: Evaluate regulatory processes and develop recommended improvements.
?? Subtask 1.8: Coordinate activities with ongoing efforts of NEI, NRC, and industry.

2.2.2 Task 2: Strengthen the Reliability Database

?? Subtask 2.1: Identify current sources of reliability data for SSCs.
?? Subtask 2.2: Identify weaknesses in sources.
?? Subtask 2.3: Improvements in reliability databases.

The primary technical responsibilities of each team participant are shown in the matrix of Table 2.2-1. The schedule for the above subtasks is shown in Figure 2.2-1.

Table 2.2-1

Primary Responsibilities of Team Participants for the Risk-Informed Project

Participant / Task	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8
Westinghouse		X		X	X	X		X
Duke Engineering	X			X				
MIT			X	X	X	X		
NCSU				X	X	X		
Egan & Associates							X	X
Sandia NL			X					
Idaho NEEL								
KOPEC*						X		

* The Korea Power Engineering Company was added as a collaborator in Phase 2, funded completely by Korean sources.

Figure 2.2-1

DOE F 4600.3
(03-94)
Replaces EIA-459B

1910-0400

U.S. DEPARTMENT OF ENERGY
FEDERAL ASSISTANCE MILESTONE PLAN

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422 - GTN, Paperwork Reduction Project (1910-0400), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-0400), Washington, DC 20503.

1. Program/Project Identification No.
DE-FC03-99SF21902, A004

2. Program/Project Title
Risk-Informed Assessment of Design and Regulatory Requirements for NPPs

3. Performer (Name, Address)
ABB Combustion Engineering Nuclear Power, Inc.
2000 Day Hill Road
Windsor, CT 06095-0500 Attn: PI Stanley Ritterbusch

4. Program/Project Start Date
8/20/99

5. Program/Project Completion Date
12/30/02

6. Identification Number	7. Planning Category (Work Breakdown Structure Tasks)	8. Program/Project Duration (1) 9/99 9/00 9/01 — S N J M M J S N J M M J S N J M M J S N	9. Comments (Notes, Name of Performer)
1.1	Identify Reg. Requirements		ABB (2)
1.2	Identify SSCs & Costs		ABB (2)
1.3	Develop Reg. Methods		ABB (2)
1.4	Dev. Simplification Methods		ABB (2)
1.5	Identify Priority SSCs		ABB (2)
1.6	Apply Methods to Sample		ABB (2)
1.7	Evaluate Reg. Process		ABB (2)
1.8	Industry Coordination		ABB (2)
2.1	Identify Data Sources		ABB (2)
2.2	Identify Data Weaknesses		ABB (2)
2.3	Develop Corrective Programs		ABB (2)

10. Remarks
(1) Two months/box (2) ABB is lead organization; collaborating orgs are Sandia, INEEL, MIT, DE&S, NCSU, Egan & Associates

11. Signature of Recipient and Date
S. E. Ritterbusch 12/20/02

12. Signature of U.S. Department of Energy (DOE) Reviewing Representative and Date

Printed with soy ink on recycled paper

3.0 Approach and Accomplishments

3.1 Task 1 Development of Risk-Informed Methodologies

3.1.1 Task 1.1 - Identify All Applicable Current Regulatory Requirements and Industry Standards

Approach

Before a new nuclear plant designer can begin to implement any methodologies for risk-informing the plant's design criteria, it is essential that the designer have a complete set of those criteria available. Thus, the objective of this task is to prepare a complete compilation of all resources for NRC criteria and industry standards that are applied to the design and operation of a typical nuclear power plant. In addition, this task will also address design criteria that are embedded in other documents. For example, NRC Regulatory Guidelines often refer to IEEE or other industry standards. Many of the criteria are embedded in documents that are not legal requirements but are, nevertheless, often applied by designers and regulators.

For this task, an assessment and compilation was made of publicly available databases and other resources for the current body of nuclear plant regulatory documentation and industry codes and standards.

Accomplishments

This task was closed in the project year ending September 30, 2001. As reported in more detail in that year's annual report, the main accomplishment of this task was a comprehensive listing of governing documents and cross-referenced documents in a database. These governing documents contain the criteria and regulations that pertain to the design, analysis and construction of a new nuclear power plant. This task also listed those national standards and codes that are routinely utilized in the design and construction process. The main product of this task is a database, developed using Microsoft Access, called Current Regulation and Industry Standards for Power Plants (CRISPP). This database identifies documents, including cross-referenced documents, from multiple data sources. This organization of data makes it possible to perform various searches and queries within the database.

The final report for this task has been published separately (Reference 1). The following paragraphs provide a summary.

The information gathered for CRISPP database was obtained from the following sources:

NUREG/CR-5973
As part of the U.S. Nuclear Regulatory Commission (NRC) Standard Review Plan Update and Development Program, Pacific Northwest Laboratory developed a listing of industry consensus codes and standards and other government and industry guidance referred to in regulatory documents, identified the latest version, and developed a summary characterization of the reference. This listing was developed from electronic searches of the Code of Federal

Regulations and the NRC's bulletins, Information Notices, Circulars, Enforcement Manual, Policy Statements, Regulatory Guides, Standard Technical Specifications, and the Standard Review Plan (NUREG-0800).

Advanced Light Water Reactor Safety Analysis Report

Combustion Engineering Standard Safety Analysis Report and the corres[ponding Design Control Document (DCD) were developed to support the NRC's Design Certoification of the System 80+ Advanced Light Water Reactor. It is structured around Regulatory Guide 1.70, Revision 3, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." The DCD also provides that design-related information be incorporated by reference in the design certification rule for the System 80+ Standard Plant Design.
The DCD is a repository of information comprising the System 80+ Standard Plant Design. The Design Control Document describes structures, systems, and components within the scope of the System 80+ Standard Plant Design, including associated programmatic provisions as specified in this document, and the requirements governing the interfaces between the System 80+ Standard Plant Design and plant-specific design features. An application for a Combined License (COL) that references the design certification rule for the System 80+ Standard Plant Design provides a plant-specific Safety Analysis Report [SAR] which include information about that part of the plant that is outside the scope of the System 80+ Standard Plant Design or which is otherwise required by a relevant provision of 10 CFR Part 52. Proprietary references, or their equivalent, that are provided in the application for design certification but not included in the DCD, must be either referenced by or included in the COL Application. Together, the Design Control Document and the plant-specific SAR provide the technically-relevant information required for a COL, or for an application for a COL, that references the design certification rule for the System 80+ Standard Plant Design. Any reference within the DCD to regulatory documentation was added to the CRISPP database.

Computer-Aided Regulatory Library (CARL)

CARL was created by the Nuclear Regulatory Expert Group at NUS Information Services, Inc. (a Scientech, Inc. company). CARL, the Computer-Aided Regulatory Library, is a PC-based reference tool – run by Folio software. CARL allows one to search the full text and abstracts of thousands of NRC documents, including full text of all NRC Notices, Generic Letters, Bulletins, Regulatory Guides, Inspection Manual, Enforcement Manual and LER abstracts, a total of more than 60 separate infobases in all. The Folio software is an information management tool which allows one to browse, search, and annotate the various infobases. One may print, highlight, add notes, build links, place bookmarks, and create groups to add value to information that is being used without altering the text of the infobase. Resulting text can be reviewed on screen, annotated, highlighted, printed, or "copied and pasted".

CRISPP Database Contents

The CRISPP database is comprised of industry consensus codes and standards gathered from the above sources into one central location. The final product will include the codes and standards cited in the following types of documents:

?? American Concrete Institute (ACI) Specifications
?? American Institute of Steel Construction (AISC) Specifications
?? American National Standards Institute (ANSI) Reports/Papers

?? American Nuclear Society (ANS) Reports / Papers
?? American Society for Testing and Materials (ASTM) Standards
?? American Society of Civil Engineers (ASCE) Journals
?? American Society of Mechanical Engineers (ASME) Papers
?? Atomic Energy Commission (AEC) Reports
?? Codes of Federal Regulations
?? Department of Transportation (DOT) Guides
?? Electric Power Research Institute (EPRI) Reports
?? Environmental Protection Agency (EPA) Manuals
?? Institute of Electrical and Electronics Engineers (IEEE) Standards / Reports
?? Instrument Society of America (ISA) Standards
?? International Commission on Radiological Protection (ICRP) Publications
?? Military Standards
?? National Council on Radiation Protection (NCRP) Reports
?? National Electrical Manufacturers Association (NEMA) Standards
?? National Fire Protection Association (NFPA) Standards
?? National Oceanic and Atmospheric Administration (NOAA) Hydrometeorlogical and Technical Reports
?? NRC Bulletins
?? NRC Circulars
?? NRC Generic Letters
?? NRC Information Notices
?? NRC Regulatory Guides and Draft Regulatory Guides
?? NRC Staff Publications (NUREGs)
?? Standard Review Plans (NUREG-0800)
?? Any other pertinent documentation necessary for the design, analysis and construction of a new nuclear power plant.

The CRISPP database is designed to assist in locating the codes and standards within a given regulatory document. It will enable one to retrieve; analyze; and perform sorts, filters, and queries on the collection of records.

3.1.2 Task 1.2 - Identify Systems, Structures, and Components (SSCs) and Their Associated Costs for a Typical Plant

Approach

Just as future plant designers will need a complete listing of design criteria for a new plant, they will also need a listing of the SSCs to which those criteria are applied. Thus, the objective of this task is to prepare such a listing for a typical nuclear plant. The list of SSCs will vary somewhat from one reactor technology to another. For example, a gas-cooled reactor would not have a Safety Injection System to pump coolant water into the reactor vessel following a pipe leak or break. To be manageable within the NERI funding levels available, the proposed research effort will need to focus upon a single type of nuclear plant, as a design that is considered typical. The regulatory requirements and industry standards (from Task 1.1) are based on Light Water Reactor (LWR) technology as are the SSCs for Task 1.2

To be able to perform a cost/benefit analysis of changes to the SSCs, future plant designers will need to know the approximate costs of the SSCs.Therefore, this task produced cost data for the typical nuclear plant, as needed, to support the efforts in the other tasks. Rather than create new cost data from scratch, this research effort modified existing available cost data, to serve as typical. The results of this task were used in Tasks 1.5 and 1.6 to identify the high priority SSCs and to apply the methodologies to a sample SSC.

Accomplishments

This task was closed in the project year ending September 30, 2001 (Reference 2). The tables below summarize the comparison of typical costs and schedules for safety-related versus non-safety-related (commercial grade) components. As expected, the schedules are longer and the costs are higher for components that are designated as *safety related* and therefore have special requirements for design, fabrication, testing and qualification. Conversely, commercial products that perform similar mechanical functions (pumping, heat transfer, and flow control or isolation) can generally be procured more quickly and cheaply.

Typical Costs for Safety and Commercial Components

	Typical Costs (Normalized)		
Component Type	**Safety Related (Notes 1, 2)**	**Non-safety/ Commercial Grade**	**Reduction for Commercial Grade**
4.1.1.1.1.1.1.1.1 Centrifugal Pumps	100	30 – 60	40 - 70%
Heat Exchangers	100	75	25%
Valves with Actuators	100	50 –60	40 - 50%
Other components - Chillers	100	20	80%
Other components - Tanks	100	50	50%
Package Units – Gas Stripper	100	40	60%

Notes:
1.Designed, fabricated, and tested in accordance with the ASME Boiler and Pressure Vessel Code, Section III, for Nuclear Power Plant Components.
2. Designed, fabricated and tested in accordance with IEEE 308, Safety Criteria for Class 1E Power Systems.

Average Procurement Schedules for Safety and Commercial Components			
	Average Procurement Schedule		
Component Type	**Safety Related (Notes 1, 2)**	**Non-safety/ Commercial Grade**	**Reduction for Commercial Grade**
Centrifugal Pumps	80 weeks	50 weeks	30 weeks (40%)
Heat Exchangers	90 weeks	45 weeks	45 weeks (50%)
Valves with Actuators	40 – 85 weeks	40 – 80 weeks	0-5 weeks (6%)
Other components - Chillers	63 weeks	45 weeks	18 weeks (30%)
Other components - Tanks	50 weeks	26 weeks	24 weeks (50%)
Package Units – Gas Stripper	110 weeks	52 weeks	58 weeks (53%)

Notes:
1. Designed, fabricated, and tested in accordance with the ASME Boiler and Pressure Vessel Code, Section III, for Nuclear Power Plant Components.
2. Designed, fabricated and tested in accordance with IEEE 308, Safety Criteria for Class 1E Power Systems.

Barriers to Using Commercial Grade Components in Safety Related Applications

The special treatment requirements that increase the procurement schedules and costs for nuclear plant components are set by regulatory and industry standards organizations. In order to achieve a significant reduction in the procurement costs and schedules of these components, changes in these requirements would be needed. This effort reviewed the high level requirements that would be affected, specifically requirements in Part 50 of Title 10 of the Code of Federal Regulations. The regulations and appendices of 10 CFR 50 that have significant impact on the cost and schedule to procure nuclear plant SSCs include:

?? 50.49, Environmental Qualification
?? 50.55a, Codes and Standards
?? App. A, General Design Criteria
?? Criterion 1, Quality standards and records
?? Criterion 2, Design bases for protection against natural phenomena
?? Criterion 3, Fire Protection
?? Criterion 4, Environmental and Dynamic Effects Design Basis
?? App. B, Quality Assurance

A discussion of these regulations and appendices and their effect on NPP component procurement cost and schedule is presented in Table 9. Designs are also affected by the more detailed requirements and guidelines in USNRC regulatory guides, standard review plans, and generic communications, and in industry standards referenced by the regulations, such as the ASME Boiler and Pressure Vessel Code.

While the added requirements for safety related systems, structures and components have produced more robust NPP designs with significant design margins for certain real and hypothetical transient events, they also tend to add significant cost to the components, sometimes without a demonstrated benefit in performance or safety. The US NRC and nuclear industry have begun a process of attempting to identify the systems, structures and components in NPPs that are more significant to the safety risk of the plant, and to modify the Special Treatment requirements accordingly.

Other Barriers and Initiatives Related to NPP Overall Cost Reduction

Other regulatory requirements that add to the overall cost of SSCs in NPPs, due to requirements for additional quantities, complexities, or capabilities, include:

?? 10 CFR 50.34, Technical Information:
Requires submittal of extensive design and analysis information in preliminary and final safety analysis reports, security and safeguards plans, and demonstration that post-TMI action items have been incorporated into the design. Post-TMI items include hardware requirements such as simulators, special display consoles, safety-related power connections for certain plant monitoring instruments, special systems analyses, and a plant-specific probabilistic risk analysis.

?? App. A, General Design Criteria
?? Criterion 17, Electric Power Systems
Requires an onsite electric power system and an offsite electric power system to permit functioning of SSCs important to safety. Each system (***assuming the other system is not functioning***) shall provide sufficient capacity and capability to assure that design limits for the boundaries that prevent radioactive material release - fuel, reactor coolant pressure boundary, and containment – are not exceeded. Assumption that either offsite or onsite system is not functioning results in two sets of power sources. Single failure criterion results in two completely redundant onsite power systems.

?? App. A, General Design Criteria
?? Criterion 34, Residual Heat Removal
?? Criterion 35, Emergency Core Cooling
?? Criterion 38, Containment Heat Removal
?? Criterion 41, Containment Atmosphere Cleanup
?? Criterion 44, Cooling Water

These criteria require that systems and components that remove residual heat from the reactor (GDC 34), provide emergency core cooling (GDC 35), remove heat from containment (GDC 38) clean up the containment atmosphere (GDC 41), and transfer heat to the ultimate heat sink (GDC 44) be powered from "safety-related" sources, i.e., can be powered from either the offsite or onsite power systems required in GDC 17, and remain functional assuming a single failure. The results are that Class 1E electrical power supplies and distribution are required for RHR, ECC, containment heat removal, containment cleanup and cooling water components, with associated increase in cost. The single failure criterion requires complete redundancy of RHR, ECC, containment heat removal, containment atmosphere cleanup, and cooling water systems and components.

?? App. A, General Design Criteria
?? Criterion 54, Piping systems penetrating containment.

- ?? Criterion 55, Reactor coolant pressure boundary penetrating containment.
- ?? Criterion 56, Primary containment isolation.
- ?? Criterion 57, Closed system isolation valves.

These criteria require that piping systems penetrating primary reactor containment have leak detection, isolation, and containment capabilities with redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating these piping systems. The piping systems must be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine if valve leakage is within acceptable limits, as part of the broader containment leak testing specified in 10 CFR 50, App. J, Containment Leakage Testing. The results are that redundant valves are required in many piping lines, Class 1E electrical power supplies are required for remote-operated containment isolation valves, and extensive testing connections must be included in the design.

Regulatory Barriers to Using Commercial Grade Components in Safety-Related Appli		
Requirement Number And Title	**Summary of Requirement(s) (taken or paraphrased from 10 CFR 50)**	**Effect Procur**
10 CFR 50.49, Environmental Qualification	Requires a qualification program to demonstrate that electrical equipment important to safety will remain functional following a postulated (assumed) accident. Qualification includes temperature, pressure, humidity, chemicals, radiation, aging, and submergence. Also requires margins beyond the expected conditions.	Compon construc testing a potentia regardle design b significa cost of c cost of p operatin design li
10 CFR 50.55a, Codes and Standards	Prescribes that pressure-retaining components in a nuclear plant must be designed, fabricated, and tested in accordance with the ASME Boiler and Pressure Vessel Code and the ASME Code for Operation and Maintenance of Nuclear Power Plants. Prescribes additional requirements on welding of Code components, records, and quality assurance.	Compon construc with ext Code. Si used to r The com requirem the cost commer (includi with oth Boiler ar as Sectio
10 CFR 50, App. A, GDC 1, Quality Standards and Records	Requires that SSCs important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.	The effe requirem Appendi
10 CFR 50, App. A, GDC 2, Design bases for protection against natural phenomena	"Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions."	The requ earthqua cost of S designed accelerat

3.1.3 Task 1.3 - Develop Methodology for Risk-Informing Requirements and Standards

Approach

The original objective for this task was to develop a set of procedures and guidelines that could be used for reviewing regulatory requirements and industry standards and revising them to be risk-informed. These procedures and guidelines would then provide a process for determining the extent to which the underlying bases for the regulation or standard are still applicable given the current state of knowledge. Further, they would provide a methodology and guidance for determining the extent to which the actual regulation or standard could be changed while still maintaining a level of safety appropriate to the underlying bases for the regulation or standard.

Early in the course of the first year's activities, it was determined that the overall objective for the task could be more readily achieved by taking a "clean sheet of paper" approach to develop a framework for *risk-based* regulation and design. This approach to developing the framework has allowed us to focus more on applying PRA techniques to address requirements for new plants without the restrictions of current NRC assumptions and acceptance criteria. Additionally, this approach provides more innovation and differentiation from the NRC's efforts on risk-informing requirements for current plants.

Accomplishments

The basic framework for a highly risk-informed design and regulatory process was developed using light-water-reactor experience. That framework was then refined to ensure it would be generic – applicable to technologies other that LWRs – using a generalized pebble-bed gas reactor was used as an example (Reference 3). A design analysis for the pebble bed reactor is summarized under Task 1.6.

The overall purpose of the new approach is to formulate a method of regulation that is logically consistent and devised so that both the reactor designer and regulator can work together in obtaining systems able to produce economical electricity safely. In this new system the traditional tools (deterministic and probabilistic analyses, tests and expert judgement) and treatments (defense-in-depth, conservatism) of safety regulation would still be employed, but the logic governing their use would be reversed from the current treatment. In the new treatment, probabilistic risk analysis (PRA) would be used as the paramount decision support tool, taking advantage of its ability to integrate all of the elements of system performance and to represent the reflects of uncertainties in these results. The latter is the most important reason for this choice, as the most difficult part of safety regulation is the treatment of uncertainties.

The scope of the PRA would be made as large as that of the reactor system, including all of its performance phenomena. The models of the PRA would be supported by deterministic analytical results and performance data to the extent feasible. However, as in the current regulatory system, the PRA models must be complemented by subjective judgements where the where the models are inadequate. All of these elements play important roles in the current decision-making structure; the main departure from current practice would be making all of these treatments explicit within the PRA, therefore, decreasing the frequency of arbitrary judgments.

In the intended sense, the PRA would be used as a vehicle for stating the beliefs of the designer and regulator. Thus, the PRA should be viewed as a Bayesian decision tool, and should be used to take advantage of its capabilities in performing an integrated assessment and in addressubg uncertainties. In order to do this, regulations must be formulated in terms of acceptable levels of unavailability of essential functions, including an acceptable level of uncertainty (e.g., the acceptability of system performance could be evaluated at a stated confidence level rather than in terms of the mean value as is typical currently).

Implied in this treatment is a hierarchy of acceptable performance goals. At the highest level societal Safety Goals would be used, supported by sub-goals formulated at increasingly fine levels of detail as the hierarchical level of the goal would decrease (see Figure1).

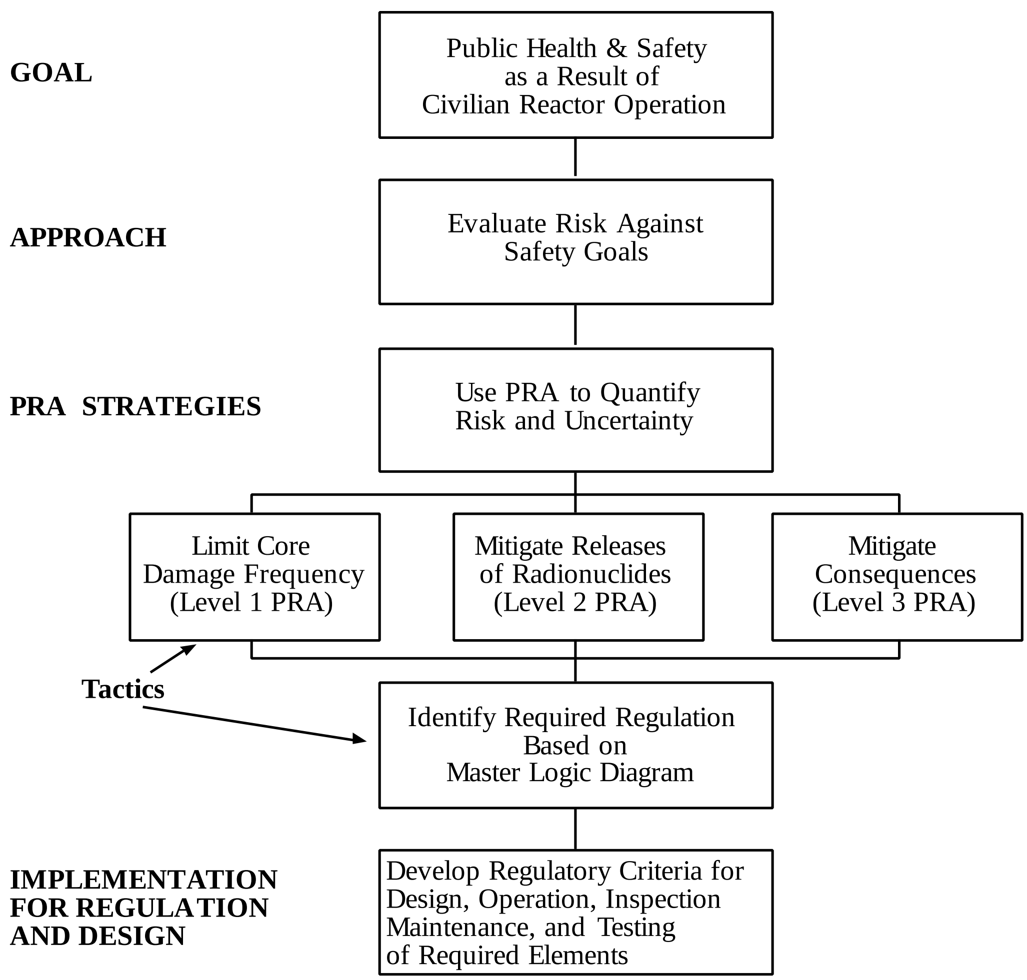

Figure 1. Framework for Risk-Based Regulation and Design

The differences between the proposed treatment and current practices are illustrated in Figure 2, which shows that the use of defense in depth and requiring performance margins would remain. However, the current practice of permitting such features to be required without justification would be abandoned; rather, wherever such a requirement were to be made it would also be necessary for the regulator to provide evidence concerning the value of the requirement and to reflect that value in the master PRA (i.e., if a redundancy is to be worth including in a system its safety value should also be stated in the overall system performance analysis).

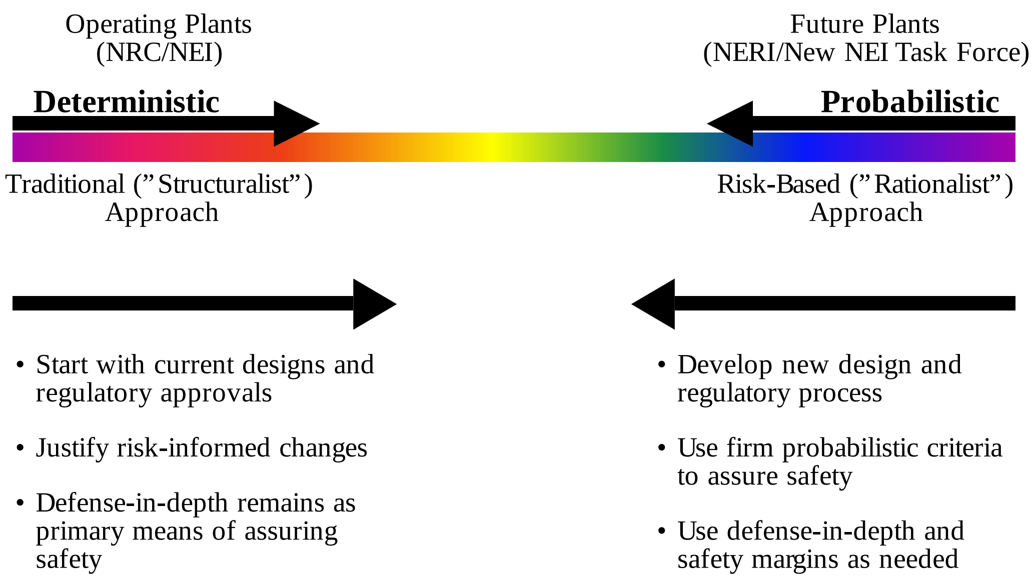

Figure 2. Comparison of NRC and NERI Risk-Informed Regulatory Processes

3.1.4 Task 1.4 - Develop Methodology for Simplifying SSCs: Risk-Based Design and Performance Evaluation of Systems, Structures, and Components

Approach

Coincident with risk-informing the regulatory framework and design bases for future nuclear plants, plant designers need a methodology for systematically reviewing the design of each and every SSC in a nuclear plant and simplifying the design to take advantage of the new risk-informed design bases. The overall goal of this effort is to reduce the costs of future nuclear plants without sacrificing safety. Since the industry standards and regulatory requirements do not literally match up with the SSCs, it is important to provide future plant designers with a methodology for cross-referencing them and assuring that the potential interactions between them are fully understood. Furthermore, because there is so much diversity in the ways that the different SSCs are designed, it will be important to have a consistent set of methodologies available to the plant designers.

The objective of this subtask is to develop a method that can be used for evaluating plant SSCs and simplifying them, using the revised requirements and standards that would result from implementation of the risk-informed design bases and regulatory framework. Inherent within this task is the need to define simplification with respect to the design of an SSC. This definition will need to address the means that can be used to "simplify' the SSC design while considering the original deterministic bases for the SSCs' design and the extent of their current relevance with respect to the SSCs' importance to safety.

In addition to developing a high level, risk-informed design process, improved and risk-based design methods for simplifying structural design were investigated.

Accomplishments

The methods for the PRA and supporting thermal-hydraulic analyses are essentially the same as those used for the System 80+ ALWR design certification program – which remain essentially "state-of-the-art" today. What is different for this project is the way in which they were used. For this project, the results from the PRA drive the decision making process, whereas for the traditional design process deterministic analyses and judgments drive the decisions and PRA is used only as an overall "investigative" tool. The use of these methods is described under Task 1.6. Work on risk-informing the design of structures and components was also advanced. This work is summarized in References 4 and 14.

Also developed was an example of an interaction with the regulator to indicate how safety issues could be resolved using the new risk-informed methodology (Reference 5). Excerpts summarizing this work are provided below.

Abstract

"The U.S. commercial nuclear industry and Nuclear Regulatory Commission currently evaluate potential regulatory reforms. At the center of these efforts to reform lies 'Risk-Informed Regulation,' a philosophy advocating the increased usage of Probabilistic Risk Assessment (PRA) for safety-related regulatory decision-making.

We study the implications of risk-based regulation in the licensing of new nuclear power plants. In particular, we investigate the current and potential roles for Design Basis Accidents (DBAs) in a risk-informed regulatory framework. The NRC ensures adequate public protection from the potential hazards of nuclear power, in part, by requiring that plants be built to withstand each DBA without loss to the systems, structures, and components necessary to assure public health and safety. Designers must demonstrate compliance with these requirements using conservative assumptions and models approved by the NRC. Prescriptive requirements for demonstrating safety disadvantage advanced reactor concepts.

The NRC currently requires use of margin in modeling and defense-in-depth features as a response to uncertainty. However, we propose the NRC should treat uncertainty quantitatively, within the context of PRA. Our proposals include use of risk-informed DBAs, a generic risk-driven design for advanced reactor concepts and a risk-informed licensing dialogue based on the plant PRA. Each of these proposals requires quantitative, probabilistic acceptability criteria and the quantitative treatment of uncertainty. In addition, we separate the evaluation of capability from that of reliability and uncertainty. We have evaluated the feasibility of these options and have conducted a simulated trial of the risk-informed licensing dialogue. We conclude that the risk-informed licensing dialogue and other risk-based regulatory tools require more comprehensive data than is currently available, as well as a standardized methodology for the consistent and accurate quantification of uncertainty.

Overview

The Nuclear Regulatory Commission (NRC) and electricity production industry seek to risk-inform regulations governing nuclear power plants, relying heavily upon the tool known as probabilistic risk assessment (PRA). This methodology provides a means of quantitatively evaluating safety, augmenting the traditional, subjective methods employed exclusively to date by the NRC and designers. In the context of these efforts, we investigate the potential role(s) for design basis accidents in a risk-informed regulatory framework. Subsequently, we propose alternatives to design basis accidents, the most credible being a risk-informed licensing dialogue, replacing the existing dialogue guidelines. In order to envision a risk-informed regulatory framework, we consider the motivation for reform and attempt to predict the characteristics of the risk-informed approach to regulation and design.

Motivations for Regulatory Reform

Considering the motivations for reform, we quickly learn that enormous capital costs and financial uncertainties associated with licensing and constructing nuclear power plants have restricted U.S. utilities from ordering any nuclear power plants in the past two decades. In the deregulated electricity market, nuclear power plants are even less economically attractive because these start-up costs hinder the possibility of a timely return on investment. On the other hand, some socio-economic factors have simultaneously increased the appeal of nuclear power as a viable option for power production. Compared to the fossil fuels used by coal, gas turbine, and natural gas plants, nuclear fuels cost utilities far less per megawatt. This disparity in cost grows each day as fossil fuels become scarcer and more expensive. Additionally, nuclear power provides electricity without the immediate environmental impacts of fossil fuel-burning plants. The U.S. government has repeatedly voiced its concern over America's growing dependence on foreign oil. Increasing electricity consumption, stricter air pollution standards and continuing unrest in the oil-rich Middle East has forced the U.S. to diversify its energy production profile. The Department of Energy and power production industry have indicated that nuclear power will continue to play a vital role in the U.S. energy profile. In order to spur new NPP construction, the start-up costs for a NPP must be reduced, while still maintaining adequate public protection.

Public opposition to nuclear power has by no means vanished but rather waned in the absence of high-profile safety incidents since Three-Mile Island. Environmental, political, and economic turmoil surrounding fossil fuels has further drawn the spotlight of criticism away from nuclear power. Additionally, the commercial nuclear power industry boasts an excellent and well-documented safety record. As a result, the nuclear power industry argues that it often endures unjustified regulatory burden without significant or demonstrable safety benefit. Accordingly, the Nuclear Regulatory Commission has accelerated efforts to re-evaluate and reform those regulations governing the licensing, construction, operation, and decommissioning of commercial nuclear power plants. The NRC hopes to reduce the enormous capital costs preventing utilities from building NPPs, while still adequately protecting the public from the unlikely, yet possible, dangers of nuclear power. Furthermore, the existing regulatory framework cannot accommodate some advanced light-water reactors (LWR) and non-LWR types currently being considered as new projects by utilities within the U.S., pending results from foreign projects. Thus, the U.S. urgently needs a new regulatory approach to licensing nuclear power plants. This improved regulatory framework must continue to ensure adequate public protection while reducing costs and providing guidance for the regulation of advanced reactor types.

Movement to 'Risk-Inform' Regulation

In recent decades, the techniques of PRA have reached a level of maturity and acceptability justifying the extensive incorporation of PRA in any new regulatory philosophy. In essence, PRA calculates the frequency (events per year) with which undesirable sequences of events will occur. We recognize that certain known combinations of low-level events (pipe breaks, valve failures, operator errors, etc) must occur in order to cause a given high-level event (core damage, radionuclide release, etc). The frequencies of high-level events can then be calculated using fault tree or event tree logic and the frequencies of low-level events. We calculate the frequencies of low-level events from historical data, traditional deterministic analyses, and expert opinion. Hence, PRA provides us with a manner for quantifying safety, rather that relying upon vague terminology such as 'not safe', 'safe enough' or 'extremely safe'.

Many industries, including the nuclear industry, have enjoyed successful experiences in applications of probabilistic decision making tools such as PRA. The South Texas Project has taken the lead in using PRA to identify those risk-significant systems, structures, and components. This program, known as Graded Quality Assurance, aims to exempt selected non-risk significant SSCs from some stringent 'special treatment' requirements (e.g. environmental qualifications). The nuclear industry continues to collect vital performance data, constantly improving the accuracy of PRA. Significant databases which aid us in assessing and predicting system and component reliability already exist. Furthermore, the nuclear industry continues to refine the science of using deterministic analyses (thermal hydraulic analyses, computer aided modeling, etc), testing and expert opinion for accurately predicting component reliability, when historical performance data are not available or applicable. Hence, PRA removes some subjectivity from the question, 'how safe is a particular NPP?' and allows us to answer the question 'how safe is safe enough?

Unfortunately, uncertainty exists concerning the accuracy of PRA estimates. The feasibility of using PRA within regulations hinges upon the evolving science of quantifying that uncertainty. Not only must we accurately calculate the frequency of an event, but we must also estimate the reasonably likely range of values that this frequency may actually take, by estimating the uncertainty surrounding our original estimate. The practical and costly alternative to an accurate quantification of uncertainty has been, and continues to be, the addition of redundant and/or diverse safety systems at the conservative and subjective discretion of the NRC staff, driven by a philosophy known as 'defense-in-depth.'

Design Basis Accidents

For example, the NRC staff, in reviewing an application to construct and operate an NPP, may require significant additions and alterations to a design before granting approval. This is generally done in response to unquantified uncertainty regarding the original design's ability to prevent 'unacceptable' events. The NRC staff effects desired plant characteristics by requiring that each proposed design can reliably mitigate design basis accidents (DBAs). The NRC defines a design basis accident as *a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety*. During the licensing process, designers must demonstrate, using approved analytical tools, that their design can survive each DBA without unacceptable radiological consequences, at the conservative and subjective discretion of the NRC staff. As we show subsequently, the current DBAs and the manner in which they are enforced, are not consistent with lessons learned from PRA.

Recall that the move to reform regulations aims to reduce capital costs while maintaining adequate safety. In this spirit, we propose an alternative to the default practice of making regulatory approval conditional upon the addition of those design features proposed by the regulator in response to uncertainty. We develop this alternative, which we call the 'Risk-Informed Licensing Dialogue', within the framework of risk-informed regulation, as an offshoot of our investigations into the potential role(s) of design basis accidents in such a framework. Unfortunately, we know very little for sure about the risk-informed regulatory framework, as it is still in development. Thus we must make assumptions.

Envisioning this framework for the future, we assume that risk-informed regulation will ensure adequate protection of the public without imposing an unjustified regulatory burden upon utilities (which ultimately becomes financial burden to consumers). In addition, such regulation will use PRA insights and capabilities wherever possible and appropriate, consistent with the NRC's PRA Policy Statement, which advocates increased use of PRA. Finally, a risk-informed regulatory framework must be applicable to advanced reactor concepts, in addition to the pressurized and boiling water reactors currently in commercial service.

Risk-Informed DBAs

We attempt to predict how design basis accidents must change in content and format in order to ensure compatibility with risk-informed regulation. In this investigation, it is necessary to highlight the benefits and weaknesses of design basis accidents (DBAs) in the existing regulatory framework. DBAs provide a level of predictability and a body of precedent for designers and regulators to use in the licensing process, from design to approval. However, designers and others suspect that DBAs, in their current state, introduce unnecessary conservatisms to the task of designing a new NPP. From these and other lessons, we develop and postulate alternate formats for DBAs using the insights from PRA. These 'risk-informed DBAs' should be more consistent with a risk-informed regulatory framework.

Unfortunately, the formulation of such a risk-informed DBA set is not a straightforward process. One must recognize that each DBA can be characterized by both its content and manner of enforcement. Using PRA, we may discover that some DBAs require the assumption that several improbable events occur simultaneously. Such a DBA might be described as having questionable content. However, that improbable DBA may 'bound' a class of more plausible accidents. It is believed that by preparing for the worst-case scenario within a certain class of accidents, an NPP's design team has addressed (or bounded) that entire class of accidents. Additionally, the manner of enforcement of DBAs provides a vital forum, within the licensing process, for regulators to address uncertainty. Thus, it may not be entirely appropriate to ignore or replace DBAs, which are shown, using PRA, to be extremely unlikely.

Alternatives to DBAs

After exploring methodologies for creating risk-informed DBA sets, we propose other avenues for capturing the benefits of DBAs, seeking to minimize the drawbacks of the existing set and their application. The existing set of DBAs, specific to LWRs, evolved as failure modes were identified through analysis and industry experience. In order to avoid this trial-and-error process for advanced reactor concepts, we explore the possibility of developing a generic risk-informed design, such that the risk-significant failure modes can be identified and considered explicitly in future designs of that reactor concept, without actually building a plant. Such a generic risk-informed design, though not developed in an optimal economic configuration, would give designers an indication of design features characteristic of a safe (by PRA standards) plant. The generic design approach has significant shortcomings and introduces a cumbersome circularity, in that the reactor concept must be proposed in detail before a risk-informed version can be developed.

After further reflection, we propose a 'risk-informed licensing dialogue,' as a replacement for the current DBA-based dialogue, or negotiation. We recognize that a DBA set may be thought of as a checklist. When a utility applies to the NRC for a license to construct and operate an NPP, the regulators look closely at the applicant's design to determine whether it satisfies all the items on the checklist. Can that design successfully and reliably mitigate all the DBAs in the prescribed set? Currently, little clear criteria exists for what constitutes 'successfully' or 'reliably.' A regulator may not feel comfortable with a design's capabilities, and may send the designer back to the drawing board. Generally, the regulators reviewing an application may indicate the need for additional design features (and, therefore, additional capital investment) in order to win regulatory approval. Meanwhile, the interest on the funds borrowed by the utility to undertake the project would compound as the designers scramble to modify their design and reformulate their original models and estimates to correspond to the modified design. This iterative process continues until the design is licensed, generally a decade later, or the parties seeking license financially collapse, as they have not begun to pay back interest or principle on the billions borrowed to undertake the project. Throughout this process, never has the following question been answered, or even stated. In terms of calculated risk, how safe is safe enough?
We propose in the risk-informed licensing dialogue that the NRC must state, in probabilistic terms, an acceptable level of safety as a basis for regulation. Regulations and regulatory practices should be consistent with this statement. This statement of safety will indicate acceptable expected values for risk metrics (measurements of risk) such as core damage frequency, release frequency or fatality frequency. In addition, the NRC must promulgate acceptable ranges and probability distributions (uncertainty) around the expected values. For instance, the NRC may state that no new plant will have an expected core damage frequency greater than 1 core damage (CD) per 10000 years and it must be 90% or more likely that the actual value will be less than 1 CD per 1000 years. We term these prescribed values

acceptability criteria. Rather than subjectively evaluating a design's compliance with individual rules (i.e. capability to mitigate individual DBAs), the NRC staff then would be required to evaluate the accuracy of the designer's overall estimates of risk and those of individual functional unreliability. We compare the regulator-certified, quantitative estimates of risk to the acceptability criteria. Since the technique of PRA is currently not mature enough to serve as the sole licensing basis, particularly in the cases of new reactor concepts, other regulatory prescriptions may be appropriate, as long as they are consistent with the NRC's probabilistic statement of acceptable calculated risk.

In this proposed approach, designers would submit a detailed design, accompanying analyses and a PRA to the regulator when seeking a license. Basic information from the completed PRA indicates whether or not the plant meets the established acceptability criteria, including those affecting allowed uncertainties. The regulator would then subjectively determine whether the detailed design and accompanying analyses justify the submitted evidence and logic structure used in the submitted PRA. In essence, the reviewing regulators would be required to ensure the accuracy and completeness of the PRA, using all available information, so that the design's risk metrics could be compared to the acceptability criteria. Regulatory approval would no longer hinges upon the inclusion of specific, regulator-chosen, additional redundant or diverse systems, which are typically selected without economic consideration.

The task of choosing appropriate systems or modifications in order to satisfy a safety requirement would remain in the hands of the designers, an economic improvement to the current system. If the regulator were to find unjustified or inaccurate data or structure used within the PRA, the regulator could then require appropriate changes to the PRA and/or supporting analyses. We would require the regulators to support and quantify their level of disagreement with designers' assertions within the context of the plant's PRA. By focusing the licensing dialogue on the design's PRA, we would provide a forum for the quantification of uncertainty. In the existing format, regulators deal with uncertainty by requiring the use of additional defense in depth and design margin. Such a requirement's safety benefit is never measured and may be illusory.

In this proposed approach, DBAs are not explicitly stated or evaluated. The set of plausible initiating events and event sequences becomes our functioning set of DBAs. We evaluate, deterministically, how a plant will respond to each of these initiators. These evaluations include thermal hydraulic modeling, computer aided simulation, testing, expert elicitation, collection of relevant historical data, human performance modeling, analysis of neutron kinetics, seismic analysis, etc… The data and conclusions of these investigations allow the designer to construct an accurate probabilistic risk assessment for that design. For the purposes of this proposal, guidance for checking the completeness of a PRA must be developed.

Evaluating the Feasibility of Alternatives

In our work, we conduct a simulation to test the feasibility of this approach. A design team submits, for regulatory review, a design and a PRA. In order to limit the scope of the simulation, we consider the function of maintaining adequate core coolant levels, as it pertains to pressurized water reactors. Our risk metric of interest is 'frequency of core damage caused by a loss-of-coolant initiator', or LOCA-CDF.

As is shown subsequently, the regulator should find unjustified data and/or structure within the initial design's PRA, then, after appropriate analysis and data alterations (the design has not been changed), the recalculated PRA could show the design to have risk metric values above acceptable values (i.e. unacceptable consequences are predicted to occur too often). The design team would return to the drawing board and be faced with a number of options for meeting the acceptability criteria. After some design modification, the PRA could again be recalculated yielding risk metric values below those of the acceptability criteria. The design and PRA could be resubmitted, gaining regulatory approval.

As we further explore the feasibility of this proposed regulatory approach, we recognize a significant increase in the amount of analysis that must be done in order to obtain accurate and complete probabilistic data. Since the current regulatory approach uses PRA as a secondary analysis tool, the task of gathering comprehensive applicable data has been somewhat neglected. As a result, PRA and data sources have yet to reach the level of requisite maturity needed for this approach. However, we also envision that eventually reliability and uncertainty in reliability will become actual specifications for sub-contractors to fill. Thus, a power plant's design team would no longer determine the frequency with which a pump would fail to start. The pump's vendor would be required to supply reliability information along with specifications for horsepower, volume output and head output. The nuclear industry would be required also to standardize the processes for expert opinion elicitation, updating reliability estimates with new test data and translating deterministic data into probabilistic estimates. Lastly, we explore the compatibility of the risk-informed licensing dialogue with other applicable guidance and regulations, such as the general design criteria (GDC).

In this work, we first identify and review the motivations for and goals of risk-based regulatory reform. Within that arena, we evaluate the potential roles for design basis accidents. After proposing alternatives to DBAs, we develop a risk-based approach to the licensing a new nuclear power plant. This approach, which we call the risk-informed licensing dialogue, replaces the use of DBAs with a forum for the quantitative handling of uncertainty (as opposed to the subjective methods currently employed). Finally, we investigate the feasibility and subtleties of this approach with an illustrative demonstration. Our feasibility investigation highlights data needs and the need for a methodology for consistently quantifying uncertainty within the context of the PRA."

3.1.5 Identify High Priority Requirements, Standards, and SSCs

Approach

Currently the NRC and industry are working to identify the regulatory requirements and SSCs that would likely yield the greatest cost savings through application of risk-informed regulation. However, these ongoing efforts are focused upon the areas that are most beneficial to reducing the operating costs of current plants. Moreover, the most beneficial areas in one nuclear plant do not necessarily match the most beneficial areas of another nuclear plant. This relates to differences in the plants' designs, as well as differences in the risk assessments that were previously performed for each of the plants.

Future plant designers, however, will need to apply the methodologies developed in Tasks 1.3 and 1.4 to all of the requirements, standards, and SSCs in a nuclear plant which are being identified in Tasks 1.1 and 1.2. This is a major undertaking and would require a budget that is well beyond the funding level of this project. This task, therefore, is limited to a review and identification of the major requirements and standards that should be analyzed in a sample application of the new risk-informed design and regulatory process.

The set of criteria established for selecting the sample application is:

- The application should be simple enough to accomplish within the resources and schedule of this project.
- The selected application should support the other tasks, for example:
  - exercise the new regulatory philosophy (Task 1.3)
  - provide a reasonably detailed application for the design methodologies (Task 1.4)
  - attract the interest and reaction of industry stakeholders - Task 1.8 (i.e., high profile, recognizable)
  - produce high potential cost reduction (Tasks 1.1, 1.2, 1.4)
  - address a reasonably significant function with potential design margin
  - be consistent with common sense/judgement
- The problem should have potential synergy with the DE&S Design/Construction NERI project and the Sandia Smart Equipment project.
- The problem should be consistent with/supportive of other on-going industry activities associated with risk informed regulation.

Accomplishments

The sample application selected based on these criteria was the RCS inventory control function. In the current plant designs, this general function encompasses a non-safety related function, the RCS makeup systems, and a safety related function, the Emergency Core Cooling System (ECCS). The ECCS design and analyses are covered by a number of standards and regulations so it provides a reasonable exercise for the risk-informed regulation methodologies from Task 1.3. The systems currently used to perform the two sub-functions have easily defined boundaries, are relatively small in scope and , as shown in Table 3.1.5-1, the ECCS is a relatively risk important system. There is a large body of knowledge available for the performance capabilities of the constituent SSCs and there is a reasonable belief that there is margin available for system simplification/refinement. Finally, there is an ongoing industry effort aimed at removing large break LOCA from the system design basis based on leak-before-break analysis. This type of design basis change would have a major impact on the design requirements for the ECCS that can be capitalized on in this project.

Table 3.1.5-1
System Risk Importance Measures For System 80 +

System Name	Risk Achievement Worth*	Risk Reduction Worth+
Emergency Feedwater System	5.01×10^{5}	2.36
Electrical Distribution System	4.01×10^{5}	1.05
Component Cooling/Station Service Water System	7.99×10^{4}	1.00
Safety Injection System	3.95×10^{4}	2.16
Safety Injection Tanks	5.01×10^{1}	1.01
Chemical and Volume Control System	1.53×10^{1}	1.02
Engineered Safety Features Actuation System	4.31×10^{3}	1.01
Shutdown Cooling System	1.27×10^{3}	1.09
Safety Depressurization System	2.89×10^{2}	1.34
Containment Spray System	1.00×10^{2}	1.00
Steam Removal System	8.85×10^{1}	1.02
Startup Feedwater System	2.82×10^{0}	1.00
Instrument Air System	1.45×10^{0}	1.00
RCS Pressure Control System	1.00×10^{0}	1.00

* The Risk Achievement Worth for a system is the ratio of the Core Damage Frequency if the system is assumed to be always failed to the base Core Damage Frequency. It is a measure of the benefit of the system or a measure of the impact of taking the system out of service

\+ The Risk Reduction Worth for a system is the ratio of the Core Damage Frequency if the system is assumed to be always available to the base Core Damage Frequency. It is a measure of the maximum potential benefit making the system perfectly reliable.

Based on Phase I results and the above criteria, the sample applications selected for analysis were the RCS inventory control and heat removal functions. The thermal-hydraulic and

Probabilistic Safety Analysis of these two functions in the context of simplifying the equipment required (i.e., a risk-informed design revision) are summarized in the following Task 1.6.

3.1.6 Apply Methodologies to a Sample SSC

Approach

In addition to providing a broad assessment of what can be accomplished by risk-informing the requirements and standards for future nuclear power plants, and then simplifying the SSCs to which they apply, an in-depth evaluation of what can be achieved must also be provided. The objective of this task is to evaluate the efficacy of the methodologies developed in Tasks 1.3 and 1.4 via a detailed trial application to a high priority SSC identified in Task 1.5. The insights gained from the trial implementation of these methodologies will then be fed back into the methodologies to improve them.

Advanced conceptual system designs for the Emergency Core Cooling System and the Emergency Feedwater System that would be capable of satisfying the Reactor Coolant System (RCS) Level Control and Heat Removal safety functions were selected to evaluate the effectiveness and feasibility of the methodologies being developed in Tasks 1, 3 and 1.4. The conceptual system is required to achieve and maintain RCS Level Control over a wide range of plant operations, from normal power operations to shutdown conditions initiated by a loss of coolant accident (LOCA) or a transient event.

For this task, the advanced conceptual systems were analyzed using best-estimate thermal hydraulic analyses to help define the event sequences and success paths. Systems based on the System 80+ design were used to estimate the risk impact on core damage frequency (CDF).

Accomplishments

Work performed in the first two years of this project is described in detail in References 18 and 19. Work performed in the third year (the final year of this project) is summarized below.

Phase 3 Thermal Hydraulic Analyses:

In the second year of this program, the Korea Power Engineering Company (KOPEC) was added as a Korea-funded collaborator. KOPEC performed the thermal-hydraulic analysis for Phase 3. This analysis supports the PSA modeling effort which was aimed at demonstrating the process for risk-informing the design of plant systems and components for advanced nuclear power plants. Literature was reviewed on the comparison of test results vs. analytical results from the MARS computer code which is based on a one-dimensional model of the reactor coolant system (RELAP5) combined with a three-dimensional model of the reactor vessel and core (COBRA) for a Large Break LOCA . The test results that were reviewed included published data from the Upper Plenum Test Facility and "direct vessel injection" tests conducted by the Korea Atomic Energy Research Institute (KAERI).

LOCA analyses were carried out for an Advanced Light Water Reactor design with new conceptual-design Emergency Core Cooling and Auxiliary Feedwater Systems as an example to "exercise" the new RIA methodology. The analyses were performed successfully, enabling the PRA model to be improved based on this more detailed verification of the PRA success criteria. Iterations between plant design, design analyses, and the PRA are a significant element of the risk-informed methodology. The three-dimensional analysis of the water injected into the reactor vessel annulus provided interesting insights into steam-water interactions, however, some trends were observed that are not completely understood. Therefore, it is recommended that further studies be undertaken to (1) evaluate the sensitivity of results to the reactor vessel nodalization scheme and its potential impact on the predicted thermal-hydraulic behavior, (2) examine the reactor core/vessel heat transfer/thermal-hydraulic model in detail and study its impact on results, and (3) evaluate the sensitivity of results to variations in significant input parameters. Further details of this work are reported in Reference 12.

Phase 3 Probabilistic Risk Analyses:

In the second year of this program, the Korea Power Engineering Company (KOPEC) was added as a Korea-funded collaborator. KOPEC performed the PSA analysis summarized in this section during Phase 3. In project year 2 of this project, the design and analysis process focused on identifying and incorporating advanced features that would meet the risk goals in a cost-effective manner. The efficacy of the RIA design method was evaluated by identifying risk-informed design changes for the System 80+ Standard Plant and evaluating the impact of these changes. The advanced conceptual design changes focused on the Emergency Core Cooling System (ECCS) and the preferred and emergency feedwater systems. The detailed functions, configurations, operations of advanced conceptual systems were based on enhancements to the System 80+ Certified design.

In the current project year, the last year of the project, a study in support of the risk assessment evaluation process was carried out based on the results of analyses performed during project year 2. Detailed breakdown of LOCA break sizes which can be mitigated by different ECCS configuration is sought in this study. Thermal-hydraulic analysis using best estimate assumptions was performed to establish the success criteria for each LOCA break size. After establishing the success criteria for each LOCA break size, risk quantification was performed. The LOCA frequencies for each break size were estimated in accordance with the method described in NUREG/CR-5750. The system fault trees and event trees generated during project year 2 were revised to develop the quantification model for LOCA break size reclassification. Further details of this work are reported in Reference 13.

Phase 3 – Risk-Informed Sample Design Analysis for Pebble Bed Gas Reactor

A sample safety analysis was performed to demonstrate that the new design and regulatory process could be applied to reactor technology other than light water reactors. The sample analysis included specification of the design configuration, use of the PRA to evaluate the design, and iterations to identify design changes that improve the overall level of safety and system reliability. Technical results, consistent with the known inherent safety features of a pebble-bed gas-cooled reactor design, indicate that a pressure-tight containment similar to those for today's operating reactors may not be required for the PBMR. While much work remains to be done to complete the design and licensing of such a gas-cooled reactor, the importance of the work completed is that the viability of the new risk-informed process has been demonstrated. This sample problem work is reported in more detail in Reference 15.

Phase 3 – Investigation of Risk-Informed Improvements to the ASME Boiler and Pressure Vessel Code

During Phase 3, work was also done to investigate the use of improved risk-informed methods to the piping design formulations in the ASME Boiler and Pressure Vessel Code. Since the completion of year 2 work on this project, there have been significant developments in the ASME committees for piping design and risk technology. Presently, a five member working group has been formed for developing Load and Resistance Factor Design (LRFD)-based ASME Section III design equations. In support of Task 1.6 of this project, North Carolina State University conducted extensive studies on developing LRFD-based design rules for piping systems. Consistent with Task 1.8 (Industry Coordination) this work is also being provided as an input to the ASME working group.

Development of structural design methodology involves consideration of safety factors to account for uncertainty in loading, material characteristics, geometrical properties, modeling, analysis, etc. Management and control of risk due to uncertainties through proper design is a major engineering goal. The design codes and standards address uncertainties through safety factors that may be defined, single-valued for a number of different combined loads such as those used for the Working Stress Design (WSD) format or explicitly for each load such as those used for the LRFD format. Currently used piping design codes such as the Section III of the American Society of Mechanical Engineers' (ASME) Boiler and Pressure Vessel and ASME B31 codes rely on the traditional WSD format in which the safety factors are prescribed deterministically. These deterministic safety factors are based on years of experience and supporting observations from test data. While the Section III rules have worked very well in practice to-date, the reliability of these designs can vary considerably leading sometimes to excessively conservative designs.

The objective is to provide useful input to the similar, but more comprehensive, study being undertaken by the ASME working group on piping design. While a complete piping system consists of several components such as straight pipes, elbows, branch connections, etc., only a cold straight pipe section is considered in this study. The performance function is defined with respect to a failure mode that is defined by plastic instability. For simplicity, only Service level D is considered and the effects of pressure and seismic moment are considered. Since the effect of dead weight is insignificant with respect to the DBE loading in service level D, it is neglected in the present study. As a first step in this process, the presently used design equation that is based on the working stress method of design is calibrated by calculating the minimum reliability levels associated with it for various values of design pressure and the diameter to thickness D/t ratio. It is observed that the minimum reliability index varies between a narrow range of 1.86 and 2.21 when mean design pressure is less than equal to $2P_a$. The *D/t* ratio has no influence on the minimum reliability levels. It is also shown that the *D/t* ratio has no influence on the partial safety factors calculated using LRFD approach. Monte Carlo simulation is used to verify the computation of partial safety factors using the First Order Reliability Method. It is illustrated that the total safety factor for the presently used design equation is same as that for a design equation based on the LRFD format in which the target reliability is equal to the minimum reliability of the presently used design equation. This work is reported in more detail in Reference 14.

Phase 3 – Addressing Uncertainties in the New Risk-Informed Design and Regulation Process

Any design process involves the requirement to address uncertainties in design models, analytical methods, material properties and equipment performance. In the past these uncertainties were addressed by adding margin to the design or adding new design features. In a highly risk-informed process, these uncertainties need to be addressed, but in the context of the PRA. That is, margin, defense-in-depth, etc. will be added when necessary in developing the PRA model. These uncertainties would arise only when there are "weaknesses" in the PRA model and, therefore, margin and defense-in-depth would be added only when justified by the quantified PRA work– not just when engineers wish to add margin to address their sometimes arbitrary judgments. This work is reported in more detail in Reference 16.

3.1.7 Evaluate Regulatory Processes and Develop Recommended Improvements

Approach

The "Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Plants" project has as one of its objectives the development of a scientific, risk-informed approach for identifying and simplifying deterministic Nuclear Regulatory Commission (NRC) requirements for nuclear power reactors that do not contribute significantly to safety. It envisions a new substantive regulatory framework that uses quantitative risk criteria and probabilistic safety assessments (PSAs).

Accomplishments

Work under Task 1.7 addressed improvements to the licensing hearing process and the NRC review process. Phase I of this task examined the NRC licensing hearing process, and recommended options for moving toward a more informal hearing process that, in contrast to the current NRC hearing process for nuclear power plant licensing, is more in line with other federal agency practice, more consistent with federal case-law in the field of administrative procedure, and more in keeping with traditional ways of resolving disputes within the scientific community, yet complies fully with statutory hearing requirements (Reference 7).

On April 16, 2001, NRC published proposed changes to its rules of practice for the conduct of hearings that were generally consistent with the Phase I Report. See 66 Fed. Reg. 19610. As of the drafting of this full Report, these changes were still pending before NRC for final approval, after consideration of the public comments received in response to the notice of proposed rule making. Phase II of the Report complements Phase I by examining possible changes to NRC's licensing framework apart from the NRC hearing process, including possible changes to NRC regulations (other than 10 CFR Part 2) and to Staff review practices. Among other things, it suggests: a new approach to resolving subjective programmatic and operational issues prior to operation under combined construction permits and operating licenses (the problem of programmatic inspection, testing, analysis, and acceptance criteria, or "programmatic ITAAC"); a new way to avoid hearing litigation over technical and financial qualifications and management integrity issues; a new method, consistent with the Atomic Energy Act, whereby the holder of an early site permit who referenced a certified design could construct a plant without having to apply for a permit from NRC; an expanded NRC backfit rule to control changes in NRC positions; a re-examination of NRC Staff's practice of issuing Safety Evaluation Reports and participating as a full party in contested nuclear power plant hearings; and a new approach to developing enforceable legislative time deadlines for NRC licensing. The Phase II investigations are reported in more detail in Reference 17.

3.1.8 Coordinate With Industry and the Nuclear Regulatory Commission

Approach

NEI, NRC, and the remainder of the nuclear industry already have underway a substantial program to develop and apply risk-informed, performance-based regulation to issues that affect the operation of the existing nuclear plants. Since the research effort for this project is intended to identify and focus on those issues that relate to the design, regulation and construction of new nuclear plants, it is essential that this project be coordinated with the already ongoing effort. Therefore, the purpose of this subtask is to interface with the NEI, NRC, and the rest of the nuclear industry. Such coordination offers several benefits. First, it avoids any unnecessary duplication of efforts between existing plant programs and new plant programs. Second, it provides access to the information on existing plant activities by the research team for this project; thus, allowing it to work more efficiently. Third, it assures that NRC, NEI, and industry consider new plant issues, in their planning. Finally, it allows the results of this proposed research effort to be used, where appropriate, to supplement activities for the existing plants.

Accomplishments

Year 1:

Westinghouse represented this project at two NRC workshops on risk-informing the current regulations for current plants (September 1999 and February 2000). The purpose of the presentation at the first workshop was to introduce our project, state its purpose of developing new methods for design and regulation of future plants, and state the importance of coordinating our project with other industry and NRC initiatives. At the second workshop, our draft regulatory framework document was summarized, with emphasis on differences (not conflicts) with the current NRC program for operating reactors.

At the Regulatory Information Conference in March 2000, Westinghuose met with representatives of NRC Research to summarize the status of our project. NEI Risk-Informed Working Group: Westinghouse attended two meetings of this working group. This project's plans were summarized, including the intent to closely coordinate activities with the ongoing

NRC effort via NEI. IAEA Consultancy Group: Westinghouse represented this project at two meetings of this working group. The purpose was to draft a report on optimizing water-cooled reactor technology. This draft was accomplished and it is consistent with and supportive of DOE's NERI program, specifically including this Risk-Informed Assessment project and its two related NERI projects for "Smart" Equipment and Improved Design and Construction methods.

Year 2:

Year 2 coordination activities included presentations to and participation in (1) the IAEA technical coordination consultancy task force and (2) the ACRS and at the Nuclear Research Safety Conference. We also supported NEI's new Task Force on the development of a generic regulatory framework for new plant designs. A slide presentation was made to the ACRS on June 2, 2001 (Reference 8). That presentation addressed the new risk-informed approach for future designs, indicating the generic portions applicable to both gas reactor and light water reactor types. It also summarized the means of expressing uncertainties in the context of probabilistic risk analyses. A paper (Reference 9) covering the same material was written and presented at the Nuclear Research Safety Conference in Washington, DC, in October 2001. We also supported NEI in their development of a white paper, sample regulations, and issues with proposed resolutions.

Year 3:

Year 3 coordination activities included support of the Nuclear Energy Institute's publication of their report on a risk-informed, performance-based regulatory process (Reference 21) and presentations at various conferences (see the last four papers listed in Section 5).

3.2 Task 2 Strengthening the Reliability Database

3.2.1 Task 2.1 - Current Sources of Reliability Data for SSCs

Approach

Current databases or published sources of reliability data that can support the development and simplification of new reactor plant designs need to be identified. The objective of this task is to identify these sources by surveying the traditional sources of data used for evaluating nuclear power plant performance and examining potential new sources of data that have not been applied to previous plant-wide risk assessments. Sources of reliability data will be identified that can be applied to new advanced technologies which will likely be utilized in new nuclear plant designs.

Each source of data will be reviewed and annotated with respect to its applicability to the current effort. Initially this effort will consist of identifying the years of experience, specific types of reliability data collected (raw data versus estimated reliability parameters), characteristics of the reliability data (failure mode, environment, quality level, unavailability versus reliability information, etc.), and applicability of data to meet NERI needs.

Accomplishments

Work for Task 2.1 is documented in Reference 18 and is summarized below.

Reliability Data Sources: Searches on reliability data associated with equipment have identified the traditional U.S. nuclear reactor failure rate databases as well several foreign database/publications. Sources of non-nuclear data have also been identified although data sources pertaining to the non-nuclear commercial sector appear to be limited. Keyword searches of the chemical and petroleum industries have turned up little information on equipment reliability databases. Searches have been performed to specifically identify digital equipment (software/hardware) reliability data. Several publications were identified that contained digital I&C reliability information, however, software reliability data appears to be very sparse. (Many references can be found that discuss methods for evaluating software reliability but there seems to be little data.)

With regard to software reliability, several potential sources of reliability data may exist in either Canadian reactors (CANDU) or British reactors (Sizewell B). There appear to be probabilistic safety assessments performed and documented on these designs. Sizewell B uses a 100,000 line computer code to automate the primary protection system, while some CANDU designs (Darlington) use software that is roughly 20 times smaller in length than the Sizewell B source code.

Reliability Database: In order to provide an efficient mechanism for users to access and perform statistical analyses using the reliability information identified, a electronic database is necessary. Some years ago the U. S. Nuclear Regulatory Commission sponsored reliability data database development effort called the Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR). Originally, NUCLARR was developed using the Modula-II programming language. Currently, the NUCLARR database is being converted into Microsoft Access format and a new user interface is being developed specifically for the NERI program application. The converted NUCLARR database contains the information (hardware and human error data) found in the original database (see NUREG/CR-4639). The NUCLARR package provides a tool that, with some modifications, will provide an analytical capability (both query capability, data aggregation, and Bayesian updating) to assess the data according to various reliability attributes.

3.2.2 Task 2.2 -Data Input Specification, Numeric Data Attributes

Approach

The database being developed (Nuclear-Application Reliability Information System - NARIS) is a collection of component and system reliability data, together with tools to select applicable data sets and generate estimates for use in risk assessment models. The database provides failure rates and probabilities of failure on demand, with associated uncertainty bounds.

Accomplishments

Work on Task 2.2 is documented in Reference 11 and is summarized below.

At its root, NARIS consists of a set of data attribute sets, each with one or more observations, and a set of methods. In subsections below, each of these sets is enumerated. That is, the possible combinations of useful numeric attributes that could be entered are listed, and the methods are listed. A third subsection provides a mapping the two, identifying which types of data are amenable to each of the methods. The data set definitions provide the information needed to accept data into the database.

The data set definitions will be given in terms of the quantitative information provided by the data sources. Various combinations of applicable information may be provided. An appendix gives protocols, or rules, for computing missing attributes and for resolving possible conflicts in the resulting data.

The algorithms for filling in the blanks specify how to calculate certain parameters from other parameters. For example, if the data source provides a median and an error factor, and the distribution is log-normal, then a mean value can be calculated. When an attribute is provided from a data source, that attribute will be stored in the database in preference to any attribute calculated from the others. If the attribute is not present, but can be inferred from the others using the specified protocol, then the inferred value will be stored in the database. The database will also contain information for each such field about whether it was inferred from the others (i.e., calculated) or was given in the data source.

A second category of protocols builds on the first. It applies to over-specification of data. If a data source provides more than the minimum number of attributes needed to define the other attributes of interest, the input computation algorithms will be used for data quality assurance. For example, as a check on the input mean from the data source, the calculated mean will be compared with the source-specified mean during the input processing. If the difference in these values exceeds 50%, the user will be notified and the data will be rejected. The user will have an opportunity to override this check if, after examining the data, the user believes that the specified mean is valid (for example, perhaps the data is very different from log-normal). The second set of protocols provides details on how these checks are to be carried out. At the time that a method is being applied, the user will be given a choice: to use the inferred values in addition to the source-provided values for the attributes required by the method, or to use only the source-provided values.

3.2.3 Task 2.3 – Improvements in the Reliability Databases

Approach

The approach for this task was to summarize current issues and propose potential improvements.

Accomplishments

The work for Task 2.3 is documented in Reference 20 and is summarized below.

Where new NPPs use SSCs similar to what is already used in current NPPs, the existing data could be collected in a manner similar to what has been done before (WASH-1400). This would entail gathering relevant data then generating probability density functions that represent the range in possible values. Representing the range of possible values is the preferred approach rather than focusing on mean values since each situation is expected to be somewhat unique in application and environment. Without detailed knowledge that a particular future application is effectively identical to some current application, it is impossible to predict which data set is the most appropriate to use; hence, the motivation for preserving range information, rather than just the expected values. However, there are a number of issues that cannot easily be addressed using existing data. These include the following:

- Human Reliability Analyses
- Physical Phenomena
- Commercial Off-The-Shelf (COTS) SSCs
- Digital Systems.

Human Reliability Analysis

Lack of data has been a weakness of every human reliability analysis (HRA) ever done. This will likely not change when HRAs are performed on new NPP designs. Nevertheless, some data does exist from actual operating experience, training exercises, and simulator experiments (Gertman and Blackman, 1994). At issue then, is how to utilize the available data for application to new NPPs. One approach to provide consistency and transportability of HRA data and analyses is the Segregated PSF Taxonomy (Appendix A of Reference 20).

Physical Phenomena

Many of the new NPP designs rely upon passive systems and processes. Often these take the form of natural circulation for decay heat removal and gravity feed to makeup to the primary coolant system. Some of the plants in the current fleet of NPPs do incorporation passive systems. Pressurized Water Reactor (PWR) designs include safety injection accumulators that operate passively. Some of the older Boiling Water Reactor (BWR) designs incorporate isolation condensers that operate using natural circulation. Neither of these systems is assumed to be 100% reliable. The ICONE-11 conference of April 20-23, 2003 included a number of papers that discuss the operation of passive systems and processes. How much confidence should be placed in passive systems and phenomena? At present, there is no quantitative data on which to base an estimate. Experiments have been conducted around the world to validate the reliance on passive phenomena for safety functions in advanced NPPs . However, there undoubtedly exist certain situations in which passive system would not function as designed. Therefore, is such situations are envisioned for specific designs, new data or assumptions and uncertainty analysis will be needed.

The first step in assessing the failure probability of passive systems is to collect any available information on actual operation of such systems. This would include both currently operating systems and experimental results. This could be used to construct bounds on the conditions that would allow passive systems to operate (and not operate). Thermal-Hydraulic code runs could also be performed to investigate various physical conditions. The aggregate of this information could be used alone to generate probability distributions, or could be used as input to an expert elicitation process.

Commercial-Off-The-Shelf Equipment

The current energy crisis has fueled renewed interest in the possibility of building new commercial NPPs. However, this interest continues to be tempered by concerns about the economic competitiveness of any proposed new NPP. This is as expected since the major barrier to expansion of the commercial nuclear power industry has always been the cost of generating electricity using a nuclear reactor compared to other means of generating electricity. The obvious truth is no utility will build a new NPP in the U.S. until they are convinced it will be economically competitive in generating electricity. The two primary concerns in this regard are the costs associated with U. S. Nuclear Regulatory Commission (NRC) licensing and construction (or capital) costs. One contributor to the capital cost issue is the cost associated with using nuclear qualified equipment versus commercial-off-the-shelf (COTS) equipment.

Some estimate the cost of qualifying equipment as safety-grade at a ten-fold increase over commercial off-the-shelf (COTS) equipment. Typically, the hardware itself is identical; the cost increase is due to the qualification tests and the documentation to certify the hardware as safety grade. The issue is whether or not this extra cost results in an actual improvement in reliability and a reduction in risk. To date, no reliability comparisons between "safety-grade" and COTS equipment have been made.

The NRC is actively engaged in an effort to risk-inform the current laws and regulations that govern the licensing and operation of NPPs. The philosophy being employed in this endeavor is that the NRC should regulate only those aspects that provide a risk-benefit to the public. The secondary objective of this approach is for the NRC to minimize the cost burden on the licensees for complying with laws and regulations that do not have a demonstrable risk-benefit. Toward this end, an effort could be made to determine if the increased cost associated with the use of nuclear-qualified equipment is justified in terms of risk-benefit.

In recent years, extensive amounts of equipment reliability data have been collected. For the current generation of NNPs, the NRC has sponsored a program at the INEEL to collect and analyze reliability data for risk-important safety systems (i.e., nuclear-grade equipment). The results of these analyses have been published in a series of NUREG/CR reports. In addition, Appendix B lists reliability information from a variety of sources both nuclear and non-nuclear. The work proposed here would use the various equipment reliability data from both NPP sources and non-nuclear sources (i.e., nuclear-grade equipment and COTS equipment), and perform comparisons to identify any correlation between the reliability performance and grade of the equipment. In this way it could be shown whether or not the nuclear-grade designation (and its associated cost) do in fact provide a risk-benefit.

Digital Systems

The reliability of digital systems is a question mark, not only for new NPP designs, but also for existing NPPs that have undergone, and continue to undergo replacement of the old analog, electro-mechanical systems. Numerous studies have been done that have generated many methods for evaluating the reliability of digital systems (Pham and Pham, 1991). However, very little data is available on the reliability of digital systems (Galyean, 1994).

It appears any single method for estimating failure rates for software suffers from some drawbacks. There will always be questions about applicability (of generic data), completeness (of a V&V), or coverage (of testing). Operational data has typically been the preferred source for estimating failure rates. However, in the case of software in a safety critical application, even this premise must be questioned. The time when the software is most needed is during some kind of abnormal upset condition of the process being controlled. Given software's deterministic nature (i.e., for identical inputs, software will always return the same output), how appropriate is it to use operational performance during normal routine conditions as an indicator of reliability.

The use of Bayes theorem simply represents one method of combining these different data sets; there are other possibilities. For example, using the four estimates described above, the highest estimate could be used to represent some arbitrary upper bound, the lowest could be used to represent a lower bound, and the two middle estimates could be combined to generate a mean value. These points could then be fit with some distribution to yield a probability density function. The approach proposed here minimizes the shortcomings of any individual method for estimating a software failure rate. By utilizing four different methods of estimating failure rates, and not relying on any single method, the chance that some aspect of software's performance will be mis-represented, is greatly reduced.

4.0 List of Deliverables and Publications

Task	Deliverable or Publication
1.1	?? "Task 1.1 - Identify All Applicable Current Regulatory Requirements and Industry Standards," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-006-2001, October 2001.
1.2	?? "Task 1.2 - Identify Systems, Structures, and Components (SSCs) and Their Associated Costs for a Typical Plant," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-007-2001, October 2001.
1.3	?? "Task 1.3 – Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants [Draft]," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-004-2000, March 2000. ?? "Task 1.3 – Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-013-2002, December 2002.
1.4	?? "Task 1.4 - Develop Methodology for Simplifying SSCs: Risk-Based Design and Performance Evaluation of Systems, Structures, and Components," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-011-2001, October 2001. ?? B.C. Beer, et. al, "Feasibility Investigations for Risk-Based Nuclear Safety Regulation,", Thesis, MIT-NSP-TR-003, February 2000.
1.5 – 1.6	?? "Task 1.6 – Thermal-Hydraulic Analyses in Support of Application of RIA Methodology to a Sample SSC, DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-009-2001, October 2001. ?? "Task 1.6 – Probabilistic Analyses in Support of Application of RIA Methodology to a Sample SSC," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-010-2001, October 2001. ?? "Task 1.6 – Thermal-Hydraulic Analyses in Support of Application of the New Risk-Informed Methodology to a Sample Problem," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-008-2002, December 2002. ?? "Task 1.6 – Probabilistic Analyses in Support of the Application of Risk-Informed Methodology to a Sample Problem," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-007-2002, December 2002. ?? "Task 1.6 - Reliability-Based Load and Resistance Factor Design for Piping: An Exploratory Case Study," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-010-2002, December 2002. ?? "Task 1.6 – Probabilistic Accident Analysis of the Pebble Bed Modular Reactor for Use With Risk-Informed Design and Regulation," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-009-2002, November 2002. ?? "Task 1.6 - Treatment of Uncertainties in a Risk-Informed Design Process," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-006-2002, December 2002.
1.7	?? "Task 1.7 - Probabilistic Safety Assessment and the Regulatory Process: Analysis of Necessary Changes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-008-2001, October 2001. ?? "Task 1.7 – Phase II – Probabilistic Risk Assessment and the Regulatory Process: Analysis of Necessary Changes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-006-2002, December 2002.
1.8	No separate deliverables – this subtask was accomplished through presentation of papers listed in this table and attendance at various meetings throughout the project (as reported in the

	annual and final reports).
2.1	?? "Task 2.1 – Reliability Databases and Reports," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-010-2000, December 2000.
2.2	?? "Task 2.2 - Database Weaknesses - Data Input Specification, Numeric Data Attributes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-005-2001, October 2001.
2.3	?? "Task 2.3 – Strengthening the Reliability Database," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-012, December 2002.
Annual Reports	?? Year 1 Annual Report, DOE Cooperative Agreement DE-FC03-99SF21902, Risk-G-007-2000, August 2000. ?? Annual Summary Report for Project Year 2, DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Risk-G-012-2001, October 2001. ?? Final Technical Report, DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Risk-G-001-2003, January 2003.
Papers	?? "An Overview of the Cooperative Program for the Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants, presented at the Korea Atomic Industrial Forum conference, Westinghouse/Ritterbusch, April 2000. ?? "Risk-Informed Assessment of Regulatory and Design Requirements for Future Nuclear Power Plants, presented at the Pacific Basin Nuclear Conference, October 2000. ?? "A Framework for Regulatory Requirements and Industry Standards for New Nuclear Power Plants," Sandia National Laboratories/Duran, presented at the PSAM-5 Conference, Osaka, Japan, November 2000. ?? "Methods for Formulation of Design Basis Accidents Within a Risk-Informed Approach to Safety Regulation of New Nuclear Power Plants," Massachusetts Institute of Technology/Golay, presented at the PSAM-5 Conference, Osaka, Japan, November 2000. ?? "A Completely New Design And Regulatory Process – A Risk-Based Approach For New Nuclear Power Plants," Westinghouse/Ritterbusch, presented at the IAEA Technology Optimization Conference, Vienna, Austria, December 2000. ?? "A New Design and Regulatory Process," NERI Project on Risk-Informed Regulation," slide presentation at the ACRS Workshop on Regulatory Challenges for Future Nuclear Power Plants, MIT/Golay, June 5, 2001. ?? "A New Risk-Informed Design and Regulatory Process," presented at the NRC's Nuclear Research Safety Conference, Washington, DC, Massachusetts Institute of Technology/Golay, October 22 – 24, 2001. ?? "Risk-Informed Licensing for Advanced Reactors," Sandia National Laboratories/Duran, presented at the PSAM-6 Conference, Puerto Rico, 2002 . ?? "Verification of Methods for Seismic Analysis of Coupled Primary-Secondary Systems With Non-Classical and Composite Modal Damping," North Carolina State University, ASME, 2002. ?? "Risk-Informed Assessment of Methodology Development and Application," presented at the ICONE-10 conference, Westinghouse/Jacob, Arlington, VA, April 2002. ?? "Risk-Informed Design of a Pebble Bed Gas Reactor," to be presented at the Korea Atomic Industrial Forum conference, Westinghouse/Ritterbusch, April 2003.

5.0 References

1. "Task 1.1 - Identify All Applicable Current Regulatory Requirements and Industry Standards," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-006-2001, October 2001.
2. "Task 1.2 - Identify Systems, Structures, and Components (SSCs) and Their Associated Costs for a Typical Plant," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-007-2001, October 2001.
3. "Task 1.3 – Framework for Risk-Based Regulation and Design for Future Nuclear Power Plants," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-013-2002, December 2002 .
4. "Task 1.4 - Develop Methodology for Simplifying SSCs: Risk-Based Design and Performance Evaluation of Systems, Structures, and Components," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-011-2001, October 2001.
5. "Methods for Formulation of Design Basis Accidents Within a Risk-Informed Approach to Safety Regulation of New Nuclear Power Plants," Massachusetts Institute of Technology, thesis report MIT-NSP-TR-003 by B. C. Beer and Prof. M. Golay, February 2000 [2001].
6. Not Used.
7. "Task 1.7 - Probabilistic Safety Assessment and the Regulatory Process: Analysis of Necessary Changes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-008-2001, October 2001.
8. MS Powerpoint presentation "NERI Project on Risk-Informed Regulation," presented at the ACRS Workshop on Regulatory Challenges for Future Nuclear Power Plants, June 5, 2001.
9. "A New Risk-Informed Design and Regulatory Process," paper presented at the NRC's Nuclear Research Safety Conference, Washington, DC, October 22 – 24, 2001.
10. "Risk-Informed Assessment Methodology – Development and Implementation," ICONE-10 Conference, Arlington, VA, April 14-18, 2002
11. "Task 2.2 - Database Weaknesses - Data Input Specification, Numeric Data Attributes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, Report RISK-G-005-2001, October 2001.
12. "Task 1.6 – Thermal-Hydraulic Analyses in Support of Application of the New Risk-Informed Methodology to a Sample Problem," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-008-2002, December 2002.
13. "Task 1.6 – Probabilistic Analyses in Support of the Application of Risk-Informed Methodology to a Sample Problem," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-007-2002, December 2002.
14. "Task 1.6 - Reliability-Based Load and Resistance Factor Design for Piping: An Exploratory Case Study," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-010-2002, December 2002.
15. "Task 1.6 – Probabilistic Accident Analysis of the Pebble Bed Modular Reactor for Use With Risk-Informed Design and Regulation,"DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-009-2002, November 2002.
16. "Task 1.6 - Treatment of Uncertainties in a Risk-Informed Design Process," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-006-2002, December 2002.

17. "Task 1.7 – Phase II - Probabilistic Risk Assessment and the Regulatory Process: Analysis of Necessary Changes," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-006-2002, December 2002.
18. "Annual Report," DOE Cooperative Agreement DE-FC03-99SF21902, Report RISK-G-007-2000, August 2000.
19. "Annual summary Report for Project Year 2," DOE Cooperative Agreement DE-FC03-99SF21902, Am. 001, October 2001.
20. "Strengthening the Reliability Database," DOE Cooperative Agreement DE-FC03-99SF21902, Am. M004, Report RISK-G-012-2002, December 2002.
21. "A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors," Nuclear Energy Institute, Report NEI 02-02, May 2002.

Appendix A: Cost and Milestone Completion Summary

Appendix A removed for this distribution.